IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2024.0429000

Unique Form and Some Construction of Uncorrelated Optimal ZCZ Sequences*

GANGSAN KIM[1], (Member, IEEE), JAEHEE NOH[2], HONG-YEOP SONG[1], (Senior Member, IEEE)
[1]Department of Electrical and Electronic Engineering, Yonsei University, Seoul, South Korea
[2]Korea Aerospace Research Institute, Daejeon, South Korea

Corresponding author: Gangsan Kim (gs.kim@yonsei.ac.kr)

This research was funded by Korea government (KASA, Korea AeroSpace Administration) grant number [RS-2022-00165802].
*This paper is an extension of our works presented at IEEE ISIT 2023 and IEEE ISIT 2024.

ABSTRACT In this paper, we first prove that any uncorrelated optimal Zero-Correlation-Zone (ZCZ) sequence family arises from Popović's construction. We then propose a new construction for such families over a polyphase alphabet. Furthermore, we establish a direct link between polyphase perfect sequences and uncorrelated optimal ZCZ sequence families: we show that if a polyphase perfect sequence can be generated by Mow's unified construction, then the corresponding uncorrelated optimal ZCZ sequence families can be generated by our proposed construction and vice versa.
In addition, we present several new properties of optimal ZCZ sequence families. For instance, we prove that the alphabet size is lower bounded by the number of sequences in the family. we also show that the interleaved sequence of an uncorrelated optimal ZCZ sequence family becomes a perfect sequence, and we conjecture the inverse when the ZCZ width is 1. Under Mow's conjecture on the alphabet size of perfect sequences, we also derive the minimal alphabet size for uncorrelated optimal ZCZ sequence families over a polyphase alphabet. Finally, we provide a simple explicit form of such minimal-alphabet families.

INDEX TERMS Optimal ZCZ sequence family, Uncorrelated sequence family, Popović's construction, Mow's conjecture on perfect sequences, Circulant Hadamard conjecture.

I. INTRODUCTION

A sequence or a sequence family with favorable correlation properties is useful in many applications including communications and cryptography [9], [11]. For a single sequence, a perfect sequence is regarded as an ideal object [5], [21]. For a sequence family, important desirable properties include uncorrelatedness among different members [2], [14], good auto-correlation of individual members [33], and the Zero-Correlation-Zone (ZCZ) property [8]. These properties are relevant not only to classical communication systems but also to synchronization, channel sounding, radar waveform design, and integrated sensing and communication systems, where low interference and reliable correlation behavior are important.

An (L, K, W)-ZCZ sequence family consists of K sequences of length L whose periodic out-of-phase auto-correlations are zero for $|\tau| < W$ and whose periodic cross-correlations are zero for $|\tau| < W$, including $\tau = 0$. Here, W is called the ZCZ width. An upper bound on K in terms of L and W is given by [32]

$$K \leq L/W.$$

When a ZCZ sequence family achieves this bound, it is called optimal. The name ZCZ first appeared in 1999 [8] but the same notion appeared much earlier by Suehiro in 1994 [31]. The ZCZ sequence families have been studied mainly for quasi-synchronous CDMA systems [2], [3], [10], [27], [34], [37], [38], and also for other communication systems including MIMO [1], [25], [29], [36]. There are many constructions for an optimal ZCZ sequence family [34], [38].

An uncorrelated ZCZ sequence family is a ZCZ sequence family with the additional property that the periodic cross-correlation is zero for any pair and at all time shifts, even outside ZCZ. The uncorrelatedness property can be beneficial for many applications. For example, in quasi-synchronous CDMA systems, uncorrelated families provide no user interference in some ideal situation. Brodzik proposed some uncorrelated ZCZ sequence families [2]. Since then, many constructions of the uncorrelated optimal ZCZ sequence family have been proposed [3], [10], [27], [37]. Interestingly, the ZCZ sequence family first proposed by Suehiro in 1994 [31] actually belongs to the uncorrelated optimal ZCZ sequence families. In this paper, we focus on Popović's construction [27], which generates an uncorrelated optimal (KW, K, W)-ZCZ sequence family from K (not necessarily distinct) perfect sequences of length W. In fact, it is one of the main results of this paper that every uncorrelated optimal (KW, K, W)-ZCZ sequence family comes from Popović's construction (Theorem 1).

In the study of the uncorrelated optimal ZCZ sequence families, many researchers have investigated the families over the polyphase alphabet [3], [10], [27], [37]. Some studies have aimed to reduce the alphabet size of the polyphase uncorrelated ZCZ sequence families [10], but no bounds on the alphabet size have been established yet.

We found some surprising properties of uncorrelated optimal ZCZ sequence families. In particular, any optimal family with parameters (KW, K, W) satisfies a property that we refer to as W-quasi-perfectness (Proposition 1). Moreover, for an uncorrelated optimal family with the same parameters, each member satisfies this property, and its periodic out-of-phase autocorrelation has constant magnitude at time shifts that are multiples of W (Proposition 2). Another property is that any optimal ZCZ sequence family with equal in-phase autocorrelation values is periodically complementary (Proposition 3), which is consistent with the relationship previously studied between ZCZ sequence families and aperiodically complementary sequences [7], [13], [16], [22]. In the proof of these properties, we are able to establish a lower bound K on the size of a polyphase alphabet over which an optimal (KW, K, W)-ZCZ sequence family exists (Corollary 2). This lower bound can be achieved only when $W = 1$. Consequently, for every nontrivial optimal (KW, K, W)-ZCZ sequence family with $W > 1$, the alphabet size must be strictly larger than K.

A perfect sequence is a sequence whose periodic autocorrelation is zero at all out-of-phase time shifts. There are several constructions of the polyphase perfect sequences [4], [6], [18], [19], [23], [24], [26], [30], and Mow unified their constructions in 1996 [21]. Mow conjectured that his unified construction could generate all the polyphase perfect sequences, and to date there has been no counterexample [30].

We propose a construction (Theorem 2) for uncorrelated optimal families of ZCZ sequences over a polyphase alphabet. Furthermore, we prove that (Remarks 6 and 7) any polyphase perfect sequence comes from Mow's unified construction if and only if any polyphase uncorrelated optimal family of ZCZ sequences comes from our proposed construction. These findings are not part of our prior work.

Mow also conjectured on the alphabet size of the polyphase perfect sequences [20], which also remains open to date. Interleaving some multiple sequences to obtain a longer one has been studied a lot [12], [38]. We are able to prove that the interleaved sequence of length K^2W from K members of an uncorrelated optimal (KW, K, W)-ZCZ sequence family becomes a perfect sequence (Corollary 1). Assuming the truth of Mow's conjecture on the alphabet size of polyphase perfect sequences, this connection gives a conjecture-dependent lower bound on the alphabet size of an uncorrelated optimal ZCZ sequence family.

We also demonstrate that (Corollary 3), by appropriately adjusting the parameters within our proposed construction in Theorem 2, some polyphase uncorrelated optimal families of ZCZ sequences with the minimum alphabet size can be constructed and represented in a simple and explicit form.

Part of the results in this paper appeared in our conference papers presented at IEEE ISIT 2023 [15] and IEEE ISIT 2024 [17]. The ISIT 2023 paper focused on several structural properties of optimal (KW, K, W)-ZCZ sequence families, which are developed in Section III of the present paper. The ISIT 2024 paper established the uniqueness result that every uncorrelated optimal (KW, K, W)-ZCZ sequence family arises from Popović's construction, which is presented in Section IV. The present journal version substantially extends these works by developing the unified construction for polyphase uncorrelated optimal ZCZ sequence families in Section V, establishing its relationship with Mow's conjectural characterization of polyphase perfect sequences, deriving new implications on minimum alphabet sizes, and further discussing the connection with the circulant Hadamard conjecture in Section VI.

This paper is organized as follows. Section II introduces notation, definitions, and known facts about the ZCZ sequence family. Section III presents structural properties of optimal ZCZ sequence families, which form the basis for the main results of this paper. Section IV proves that Popović's construction generates all uncorrelated optimal ZCZ sequence families. Section V proposes a construction for polyphase uncorrelated optimal ZCZ sequence families and explores its relationship with Mow's unified construction. Section VI discusses a connection with the circulant Hadamard conjecture, first stated by Ryser [28]. In particular, if a circulant Hadamard matrix of order K^2 exists for $K > 2$, then its top row is a binary perfect sequence of length K^2. We study a deinterleaving condition under which this would yield an uncorrelated optimal $(K, K, 1)$-ZCZ sequence family (Conjecture 3), and verify this condition for all known polyphase perfect sequences of length K^2, including Fermat-quotient sequences of length p^2 (Proposition 4).

II. PRELIMINARIES

We will fix the following notation throughout the paper.

- $\mathbb{Z}$ is the set of integers and $\mathbb{C}$ is the set of complex numbers.
- $\mathbb{Z}_L$ is the integers mod L. $u\mathbb{Z}_L$ denotes the multiples of u in $\mathbb{Z}_L$.
- We use $n \pmod{L}$ to mean the integer x in the range $0 \le x < L$ such that $x \equiv n \pmod{L}$.
- A sequence of length L is denoted by $\boldsymbol{a} = \{a(t) \mid t \in \mathbb{Z}_L\}$, where $a(t+L) = a(t)$ for all t. We also regard $\boldsymbol{a}$ as the row vector $(a(0), a(1), \ldots, a(L-1))$ when convenient. Unless otherwise specified, all sequences are complex-valued.
- For a sequence $\boldsymbol{a} = \{a(t) \mid t \in \mathbb{Z}_L\}$, its conjugate sequence is $\boldsymbol{a}^* = \{a^*(t) \mid t \in \mathbb{Z}_L\}$. For a constant λ,

we write $\lambda \boldsymbol{a} = \{\lambda a(t) \mid t \in \mathbb{Z}_L\}$.

- For two sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ of length L, their term-by-term product is denoted by $\boldsymbol{a} \circledast \boldsymbol{b}$, where

$$(\boldsymbol{a} \circledast \boldsymbol{b})(t) \triangleq a(t)b(t), \quad t \in \mathbb{Z}_L.$$

Their term-by-term sum is denoted by $\boldsymbol{a} + \boldsymbol{b}$.

- For two sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ of length L, their periodic correlation is

$$C(\boldsymbol{a}, \boldsymbol{b}; \tau) \triangleq \sum_{t \in \mathbb{Z}_L} a(t+\tau)b^*(t), \quad \tau \in \mathbb{Z}_L,$$

where $t+\tau$ is computed modulo L. We write $C(\boldsymbol{a}, \boldsymbol{b}; \cdot)$ for the corresponding correlation sequence. When $\boldsymbol{a} \neq \boldsymbol{b}$, it is called the cross-correlation. When $\boldsymbol{a} = \boldsymbol{b}$, it is called the auto-correlation and is denoted by $C(\boldsymbol{a}; \tau)$ or $C(\boldsymbol{a}; \cdot)$.

- $\omega_v \triangleq e^{\frac{2\pi}{v}\sqrt{-1}}$ is a primitive v-th root of unity over $\mathbb{C}$.
- A root-of-unity sequence is a complex sequence over an alphabet contained in the unit circle. It is called polyphase if its alphabet is a regular polygon on the unit circle. A polyphase sequence has alphabet size v if the alphabet is the set of integer powers of ω_v.
- A pair of sequences is said to be uncorrelated if their cross-correlation becomes zero at all time-shifts. A family of sequences is said to be uncorrelated if every pair is uncorrelated.
- A sequence is perfect if its auto-correlation is zero at all nonzero shifts. A sequence $\boldsymbol{a}$ of length KW is W-quasi-perfect if

$$C(\boldsymbol{a}; \tau) = 0 \quad \text{whenever} \quad \tau \notin W\mathbb{Z}_{KW}.$$

A family $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{M-1}\}$ of length-KW sequences is W-quasi-perfect if each member is W-quasi-perfect and, for $0 \leq i < j < M$,

$$C(\boldsymbol{a}_i, \boldsymbol{a}_j; 0) = 0 \quad \text{and} \quad C(\boldsymbol{a}_i, \boldsymbol{a}_j; \tau) = 0 \quad \text{whenever} \quad \tau \notin W\mathbb{Z}_{KW}.$$

- A sequence family $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{K-1}\}$ all of length L is said to be periodically complementary if

$$\sum_{i=0}^{K-1} C(\boldsymbol{a}_i; \tau) = 0 \quad \text{for } \tau \neq 0.$$

- For a sequence $\boldsymbol{a} = \{a(t) \mid t \in \mathbb{Z}_L\}$, its DFT sequence is

$$(\mathrm{DFT} \circ \boldsymbol{a})(n) = \frac{1}{\sqrt{L}} \sum_{j \in \mathbb{Z}_L} \omega_L^{jn} a(j), \quad n \in \mathbb{Z}_L.$$

For a sequence $\boldsymbol{b} = \{b(n) \mid n \in \mathbb{Z}_L\}$, its IDFT sequence is

$$(\mathrm{IDFT} \circ \boldsymbol{b})(t) = \frac{1}{\sqrt{L}} \sum_{j \in \mathbb{Z}_L} \omega_L^{-jt} b(j), \quad t \in \mathbb{Z}_L.$$

- For an integer M, the M-fold-expander E_M maps a length-L sequence $\boldsymbol{a}$ to a length-ML sequence defined by

$$(\mathrm{E}_M \circ \boldsymbol{a})(t) = \begin{cases} a(t/M) & \text{for } t \in M\mathbb{Z}_{ML}, \\ 0 & \text{otherwise.} \end{cases}$$

- For $i \in \mathbb{Z}_L$, the cyclic shift operator T^i is defined by

$$(\mathrm{T}^i \circ \boldsymbol{a})(t) = a(t+i), \quad t \in \mathbb{Z}_L.$$

- For sequences $\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{M-1}$ of length L, their interleaved sequence is

$$\mathcal{I}(\boldsymbol{a}_0; \boldsymbol{a}_1; \cdots; \boldsymbol{a}_{M-1}) \triangleq \boldsymbol{a} = \{a(t) \mid t \in \mathbb{Z}_{ML}\},$$

where

$$a(t) = a(qM+h) = a_h(q),$$

and q and h are the quotient and the remainder when t is divided by M.

Known fact 1 ([21]): Let $\mathcal{A} = \{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots \boldsymbol{a}_{K-1}\}$ be an uncorrelated and periodically complementary sequence family all of same length. Then,

$$\mathcal{I}(\boldsymbol{a}_0; \boldsymbol{a}_1; \cdots; \boldsymbol{a}_{K-1})$$

is a perfect sequence.

We use the following standard DFT properties [35].

Known fact 2 (Properties of DFT [35]): Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be complex-valued sequences of length L. Then the following is true:

1) For the periodic correlation sequence $C(\boldsymbol{a}, \boldsymbol{b}; \cdot)$,

$$\frac{1}{\sqrt{L}}(\mathrm{DFT} \circ C(\boldsymbol{a}, \boldsymbol{b}; \cdot)) = (\mathrm{DFT} \circ \boldsymbol{a}) \circledast (\mathrm{DFT} \circ \boldsymbol{b})^*.$$

Consequently, $\boldsymbol{a}$ and $\boldsymbol{b}$ are uncorrelated if and only if $(\mathrm{DFT} \circ \boldsymbol{a}) \circledast (\mathrm{DFT} \circ \boldsymbol{b})^*$ is the all-zero sequence. Also, $\boldsymbol{a}$ is perfect if and only if

$$|(\mathrm{DFT} \circ \boldsymbol{a})(n)| = |(\mathrm{DFT} \circ \boldsymbol{a})(0)| \quad \text{for} \quad n \in \mathbb{Z}_L.$$

2) For $n, t \in \mathbb{Z}_L$,

$$(\mathrm{DFT} \circ (\mathrm{T}^i \circ \boldsymbol{a}))(n) = \omega_L^{-in} (\mathrm{DFT} \circ \boldsymbol{a})(n),$$
$$(\mathrm{IDFT} \circ (\mathrm{T}^i \circ \boldsymbol{a}))(t) = \omega_L^{+it} (\mathrm{IDFT} \circ \boldsymbol{a})(t).$$

3) For $n, t \in \mathbb{Z}_{ML}$,

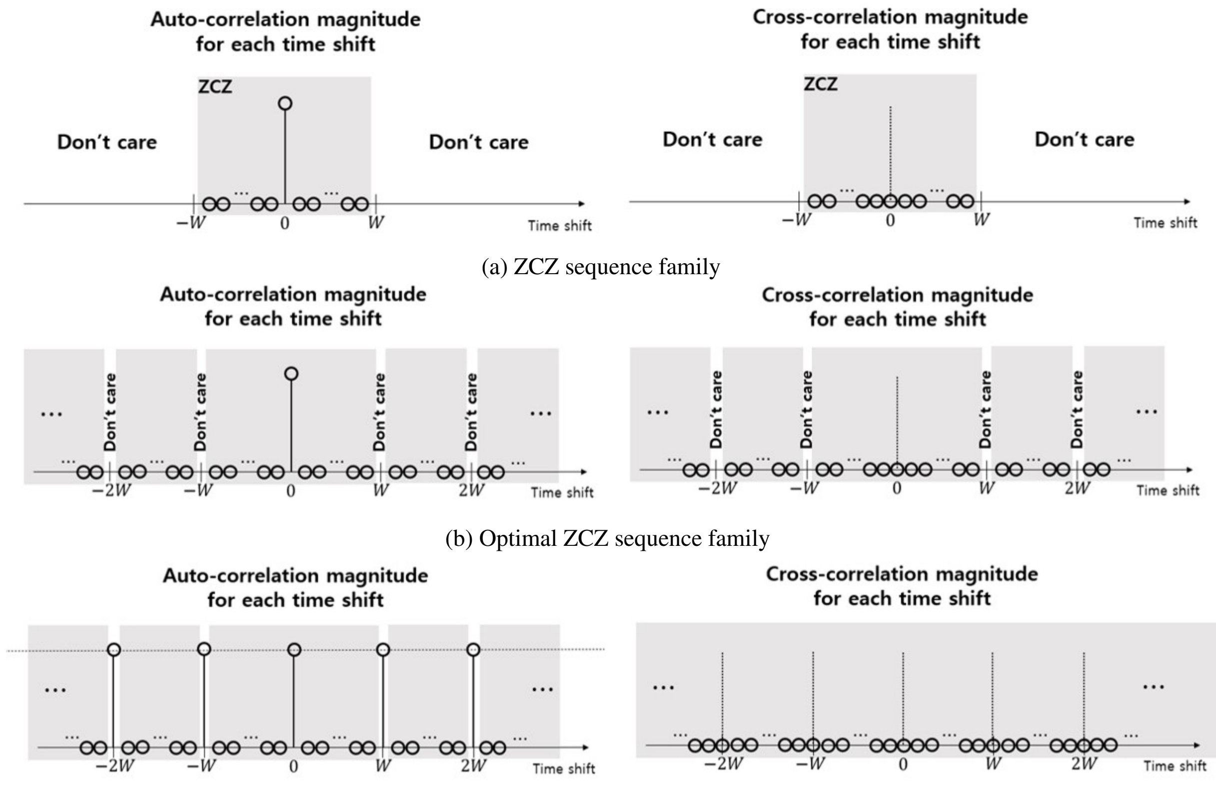
$$(\mathrm{DFT} \circ (\mathrm{E}_M \circ \boldsymbol{a}))(n) = \frac{1}{\sqrt{M}} (\mathrm{DFT} \circ \boldsymbol{a}) (n \pmod{L}),$$
$$(\mathrm{IDFT} \circ (\mathrm{E}_M \circ \boldsymbol{a}))(t) = \frac{1}{\sqrt{M}} (\mathrm{IDFT} \circ \boldsymbol{a})(t \pmod{L}).$$

Known fact 3 (ZCZ sequence family and Optimality [32]): Let $\mathcal{A} = \{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{K-1}\}$ be a set of K sequences all of length L.

1) (Definition) The set $\mathcal{A}$ is called an (L, K, W)-ZCZ sequence family if for any i and j

$$C(\boldsymbol{a}_i, \boldsymbol{a}_j; \tau) = 0 \quad \text{for} \quad |\tau| < W,$$

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2026.3724501



(a) ZCZ sequence family

(b) Optimal ZCZ sequence family

(c) Uncorrelated optimal ZCZ sequence family

FIGURE 1: General correlation magnitude of (a) ZCZ sequence family, (b) optimal ZCZ sequence family and (c) uncorrelated optimal ZCZ sequence family (ZCZ width is W in all cases)

except for the case of $\tau = 0$ and $i = j$. Here, W is called the ZCZ width.

2) (Bound and Optimality) For an (L, K, W)-ZCZ sequence family, the following inequality holds:

$$K \le L/W.$$

When the equality is achieved, the family is called optimal.

Remark 1: A ZCZ sequence family is called uncorrelated if the members are uncorrelated sequences. The above bound also applies to uncorrelated ZCZ sequence family and the family is called an uncorrelated optimal ZCZ sequence family when the equality is achieved. We are mainly interested in the uncorrelated optimal ZCZ sequence family in this paper.

III. PROPERTIES OF OPTIMAL ZCZ SEQUENCE FAMILY

The correlations of a ZCZ sequence family having the ZCZ width W are depicted in Figure 1-(a). This family will be a W-quasi-perfect sequence family if the ZCZ width W repeats periodically. Therefore, a W-quasi-perfect sequence family is inherently a ZCZ sequence family but not conversely. It is surprising that an optimal ZCZ sequence family is always a W-quasi-perfect sequence family as shown in Figure 1-(b).

Proposition 1: An optimal ZCZ sequence family with ZCZ parameter (KW, K, W) is a W-quasi-perfect sequence family.

Proof: Consider an optimal (KW, K, W)-ZCZ sequence family

$$\mathcal{A} = \{\boldsymbol{a}_0, \boldsymbol{a}_1, ..., \boldsymbol{a}_{K-1}\}.$$

We consider i-shift of every member of it. That is, let

$$\mathcal{A}_i \triangleq \{\mathrm{T}^i \circ \boldsymbol{a}_0, \mathrm{T}^i \circ \boldsymbol{a}_1, ..., \mathrm{T}^i \circ \boldsymbol{a}_{K-1}\}$$

for $i = 0, 1, ..., KW - 1$. Note that $\mathcal{A}_0 = \mathcal{A}$. It is now sufficient to show that any member of $\mathcal{A}_0$ is orthogonal to all the members in $\mathcal{A}_\tau$ for $\tau \notin W\mathbb{Z}_{KW}$, which is our main claim for this proof. Here, we may consider the members in $\mathcal{A}_i$ as row vectors of length KW.

To prove the claim, we consider any consecutive index set $\mathcal{I} \subset \mathbb{Z}_{KW}$ of size W and consider KW vectors in $\bigcup_{i \in \mathcal{I}} \mathcal{A}_i$. We observe that any two vectors here are orthogonal to each other, from the definition of ZCZ property of the family $\mathcal{A}$, since their inner product is a correlation of sequences in $\mathcal{A}$ at time shift $|\tau| < W$. Therefore, the set $\bigcup_{i \in \mathcal{I}} \mathcal{A}_i$ becomes an orthogonal basis of $\mathbb{C}^{KW}$.

We now consider the linear space $\mathbb{B}_i$ spanned by the vectors in $\mathcal{A}_i$ for $i = 0, 1, ..., KW - 1$. From the above observation, we see that, for any $i \neq j$ both in $\mathcal{I}$, we have $\mathbb{B}_i \perp \mathbb{B}_j$ since $\mathcal{A}_i \perp \mathcal{A}_j$. Furthermore, we also have, for any $\kappa \in \mathcal{I}$,

$$\mathbb{B}_\kappa \perp \mathbb{B}_j \quad \text{for} \quad j \in \mathcal{I} \backslash \{\kappa\},$$

or, in particular, we have

$$\mathbb{B}_0 \perp \mathbb{B}_j \quad \text{for} \quad j \in \{1, 2, ..., W-1\}. \tag{1}$$

Furthermore, we observe that

$$\mathbb{B}_\kappa = \left(\operatorname{span}\left(\bigcup_{i \in \mathcal{I} \setminus \{\kappa\}} \mathcal{A}_i\right)\right)^\perp, \tag{2}$$

where $(\cdot)^\perp$ denotes the orthogonal complement of $(\cdot)$ in $\mathbb{C}^{KW}$. Therefore, using $\mathcal{I}_\tau = \{\tau, \tau+1, ..., \tau+W-1\}$, LHS $\mathbb{B}_\tau$ in (2) with $\kappa = \tau$ becomes

$$\mathbb{B}_\tau = \left(\operatorname{span}\left(\bigcup_{i \in \mathcal{I}_\tau \setminus \{\tau\}} \mathcal{A}_i\right)\right)^\perp.$$

Using $\mathcal{I}' = \mathcal{I}_\tau + 1 = \{\tau+1, \tau+2, ..., \tau+W\}$, LHS $\mathbb{B}_{\tau+W}$ in (2) with $\kappa = \tau + W$ becomes

$$\mathbb{B}_{\tau+W} = \left(\operatorname{span}\left(\bigcup_{i \in \mathcal{I}' \setminus \{\tau+W\}} \mathcal{A}_i\right)\right)^\perp.$$

We observe that RHS of both of the above are the same, since $\mathcal{I}_\tau \setminus \{\tau\} = \mathcal{I}' \setminus \{\tau+W\}$. Therefore, we have

$$\mathbb{B}_\tau = \mathbb{B}_{\tau+W}.$$

In general, similarly, we have,

$$\mathbb{B}_\tau = \mathbb{B}_{\tau \pmod W} \quad \text{for any } \tau \in \mathbb{Z}_{KW}. \tag{3}$$

Finally, the claim is proved by (1) and (3). ∎

The second property comes when the optimal ZCZ sequence family is in fact uncorrelated. Observe the notation "Don't care" in Figure 1-(b). It means either we don't care for the value there or in fact we do not know the value there. For an uncorrelated optimal ZCZ sequence family, this value is zero for cross-correlation (from the definition of uncorrelatedness) and it is the same as the in-phase value for auto-correlation as shown in Figure 1-(c).

Proposition 2: Let $\mathcal{A} = \{\boldsymbol{a}_i | i = 0, 1, ..., K-1\}$ be an uncorrelated optimal (KW, K, W)-ZCZ sequence family. Then, each member $\boldsymbol{a}_i$ is W-quasi-perfect and

$$|C(\boldsymbol{a}_i; \tau)| = C(\boldsymbol{a}_i; 0) \quad \text{for } \tau \in W\mathbb{Z}_{KW}.$$

Proof: It would be sufficient to show that, for every i, there exists an integer $\kappa(i)$ such that

$$a_i(t+W) = \omega_K^{\kappa(i)} a_i(t) \quad \text{for} \quad t \in \mathbb{Z}_{KW}. \tag{4}$$

Indeed, this implies that, for $\tau = jW$,

$$\begin{aligned} C(\boldsymbol{a}_i; \tau) &= \sum_t a_i(t+jW) a_i^*(t) \\ &= \omega_K^{j\kappa(i)} C(\boldsymbol{a}_i; 0). \end{aligned} \tag{5}$$

Without loss of generality, we prove (4) for $i = 0$. For any subset $\mathcal{I} \subset \mathbb{Z}_{KW}$ and $j \in \{0, 1, \dots, K-1\}$, let

$$\mathcal{S}(\mathcal{I}; j) \triangleq \{\mathrm{T}^i \circ \boldsymbol{a}_j \mid i \in \mathcal{I}\}.$$

For any K subsets $\mathcal{I}_0, \mathcal{I}_1, \dots, \mathcal{I}_{K-1} \subset \mathbb{Z}_{KW}$, each consisting of W consecutive indices, define

$$\mathcal{S} \triangleq \bigcup_{j=0}^{K-1} \mathcal{S}(\mathcal{I}_j; j).$$

Any two distinct vectors in $\mathcal{S}$ are orthogonal: if they come from different members, their inner product is a cross-correlation and is zero by uncorrelatedness; if they come from the same member, their inner product is an out-of-phase auto-correlation at a shift of magnitude less than W and is zero by the ZCZ property. Thus, $\mathcal{S}$ is an orthogonal basis of $\mathbb{C}^{KW}$. Therefore, for any $i_0 \in \mathcal{I}_0$,

$$\operatorname{span}(\{\mathrm{T}^{i_0} \circ \boldsymbol{a}_0\}) = \left(\operatorname{span}\left(\mathcal{S} \setminus \{\mathrm{T}^{i_0} \circ \boldsymbol{a}_0\}\right)\right)^\perp. \tag{6}$$

Now choose

$$\mathcal{I}_j = \{0, 1, \dots, W-1\} \quad \text{for } j = 1, \dots, K-1.$$

For the first member, compare the two choices

$$(\mathcal{I}_0, i_0) = (\{0, 1, \dots, W-1\}, 0)$$

and

$$(\mathcal{I}_0, i_0) = (\{1, 2, \dots, W\}, W).$$

In both cases, the right-hand side of (6) is

$$\left(\operatorname{span}\left(\begin{array}{c}\bigcup_{j=1}^{K-1} \mathcal{S}(\{0, 1, \dots, W-1\}; j) \\ \cup \mathcal{S}(\{1, 2, \dots, W-1\}; 0)\end{array}\right)\right)^\perp.$$

Therefore, both $\boldsymbol{a}_0$ and $\mathrm{T}^W \circ \boldsymbol{a}_0$ lie in the same one-dimensional subspace, and hence $\boldsymbol{a}_0 = \lambda(\mathrm{T}^W \circ \boldsymbol{a}_0)$ for some $\lambda \in \mathbb{C}$. Thus,

$$a_0(t) = \lambda a_0(t+W) \quad \text{for} \quad t \in \mathbb{Z}_{KW}.$$

Iterating this relation K times gives

$$a_0(t) = \lambda^K a_0(t+KW) = \lambda^K a_0(t).$$

Hence $\lambda^K = 1$, so there exists an integer κ such that $\lambda = \omega_K^\kappa$. This proves (4). ∎

Two propositions so far will be used to prove the uniqueness of an uncorrelated optimal ZCZ sequence family in Section IV as Theorem 1.

The third property is that any (correlated or uncorrelated) optimal ZCZ sequence family is periodically complementary. For this, we have to assume that the in-phase auto-correlation values of all the members are the same.

Proposition 3: Let $\mathcal{A} = \{\boldsymbol{a}_i | i = 0, 1, ..., K-1\}$ be an optimal (KW, K, W)-ZCZ sequence family and we assume that $C(\boldsymbol{a}_0; 0) = C(\boldsymbol{a}_1; 0) = \cdots = C(\boldsymbol{a}_{K-1}; 0)$, where $C(\boldsymbol{a}_i; 0)$ is the in-phase auto-correlation value of $\boldsymbol{a}_i$. Then, $\mathcal{A}$ is a periodically complementary sequence family.

Proof: Without loss of generality, assume that

$C(\boldsymbol{a}_0;0)=1$. For $i=0,1,...,K-1$, let S_i be a $W\times KW$ matrix given by

$$S_i \triangleq \begin{bmatrix} \boldsymbol{a}_i \\ \mathrm{T}^1\circ \boldsymbol{a}_i \\ \mathrm{T}^2\circ \boldsymbol{a}_i \\ \vdots \\ \mathrm{T}^{W-1}\circ \boldsymbol{a}_i \end{bmatrix},$$

where the j-th row is the row vector $\boldsymbol{a}_i$ shifted by j times to the left for $j=0,1,...,W-1$. Let S be a $KW\times KW$ square matrix given by

$$S \triangleq \begin{bmatrix} S_0 \\ S_1 \\ \vdots \\ S_{K-1} \end{bmatrix}.$$

By definition of ZCZ sequence family, all the rows of S are orthogonal to all others. Therefore, by assumption $C(\boldsymbol{a}_0;0)=1$, S is a unitary matrix so that the orthogonality applies also to the columns of S. Note that t-th column of S is

$$\begin{aligned}
&(a_0(t),a_0(t+1),...,a_0(t+W-1),\\
&\ a_1(t),a_1(t+1),...,a_1(t+W-1),\\
&\ \ldots\ldots,\\
&\ a_{K-1}(t),...,a_{K-1}(t+W-1))^{\mathsf{T}}.
\end{aligned}$$

For any t_1 and any $\tau\neq 0$, the orthogonality between t_1-th column and $(t_1+\tau)$-th column of S implies

$$\sum_{i=0}^{K-1}\sum_{t=t_1}^{t_1+W-1} a_i(t+\tau)a_i^*(t)=0.$$

Therefore, for any $\tau\neq 0$,

$$\begin{aligned}
\sum_{i=0}^{K-1} C(\boldsymbol{a}_i;\tau) &= \sum_{i=0}^{K-1}\sum_{t\in\mathbb{Z}_{KW}} a_i(t+\tau)a_i^*(t)\\
&= \sum_{i=0}^{K-1}\sum_{t_1\in W\mathbb{Z}_{KW}}\sum_{t=t_1}^{t_1+W-1} a_i(t+\tau)a_i^*(t)\\
&= \sum_{t_1\in W\mathbb{Z}_{KW}}\sum_{i=0}^{K-1}\sum_{t=t_1}^{t_1+W-1} a_i(t+\tau)a_i^*(t)\\
&= \sum_{t_1\in W\mathbb{Z}_{KW}} 0 = 0.
\end{aligned}$$

Therefore, $\mathcal{A}$ is a periodically complementary sequence family. ■

We recall **Known fact 1** which says that the interleaved sequence of the uncorrelated and periodically complementary sequence family is a perfect sequence. Now, an optimal ZCZ sequence family is (surprisingly) a periodically complementray sequence family. If it is uncorrelated, then the interleaving will result in a perfect sequence.

Corollary 1: Let $\mathcal{A}=\{\boldsymbol{a}_i|i=0,1,...,K-1\}$ be an uncorrelated optimal (KW,K,W)-ZCZ sequence family with $C(\boldsymbol{a}_0;0)=C(\boldsymbol{a}_1;0)=\cdots=C(\boldsymbol{a}_{K-1};0)$. Then, the interleaved sequence $\mathcal{I}(\boldsymbol{a}_0;\boldsymbol{a}_1;\boldsymbol{a}_2;\cdots;\boldsymbol{a}_{K-1})$ of length K^2W is a perfect sequence.

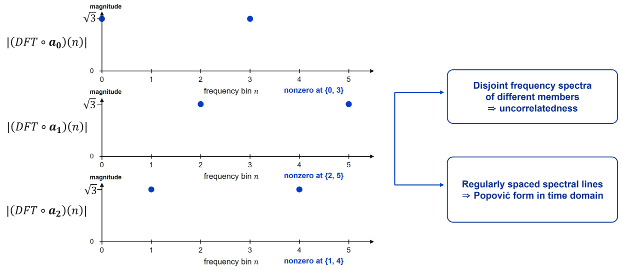


FIGURE 2: Frequency-domain illustration of uncorrelated optimal ZCZ sequence family members for $K=3$ and $W=2$

IV. UNIQUE FORM OF THE UNCORRELATED OPTIMAL ZCZ SEQUENCE FAMILY

In 2018, Popović proposed the construction of the uncorrelated optimal ZCZ sequence families [27]. In 2022, Fang and Wang demonstrated that Popović's construction could be simply expressed as the following **Known fact 4** [10].

Known fact 4 (Popović's construction [10], [27]): For some positive integers K and W, let $\boldsymbol{g}_i=\{g_i(t)|t\in\mathbb{Z}_W\}$ for $i=0,1,...,K-1$ be some arbitrary (not necessarily distinct) perfect sequences all of length W. Construct a family of sequences $\boldsymbol{a}_i=\{a_i(t)|t\in\mathbb{Z}_{KW}\}$ for $i=0,1,...,K-1$ all of length KW by:

$$a_i(t)=g_i(t \pmod W)\omega_{KW}^{it} \quad \text{for} \quad t\in\mathbb{Z}_{KW}. \tag{7}$$

Then, the sequence family $\mathcal{A}=\{\boldsymbol{a}_i|i=0,1,...,K-1\}$ where $\boldsymbol{a}_i=\{a_i(t)|t\in\mathbb{Z}_{KW}\}$ is an uncorrelated optimal (KW,K,W)-ZCZ sequence family.

The following is one of the main results of this paper.

Theorem 1 (Unique Form): Every uncorrelated optimal (KW,K,W)-ZCZ sequence family comes from the Popović's construction described in **Known fact 4**.

Before giving the proof, Fig. 2 gives a frequency-domain interpretation of the main idea. It illustrates the case $K=3$ and $W=2$. The three members have nonzero spectral components on the disjoint frequency-bin sets

$$\{0,3\},\qquad \{2,5\},\qquad \{1,4\},$$

respectively, and each nonzero spectral magnitude is $\sqrt{3}$ under the unitary DFT normalization used in this paper. The disjointness of these spectra accounts for the uncorrelatedness of different members, while the regular spacing of the nonzero spectral components reflects the Popović form in the time domain. The proof below makes this intuition precise by using Propositions 1 and 2 to derive this forced spectral structure and then showing that the corresponding component sequences are perfect.

Proof: Assume that we are given an uncorrelated optimal (KW,K,W)-ZCZ sequence family $\mathcal{A}=\{\boldsymbol{a}_0,\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{K-1}\}$, where $\boldsymbol{a}_i=\{a_i(t)\mid t\in\mathbb{Z}_{KW}\}$ for $i=0,1,\ldots,K-1$. It is sufficient to show that the family $\mathcal{A}$ can be represented as shown in (7).

By Proposition 2, for each i there exists an integer $\kappa(i)$ such that

$$a_i(t+W) = \omega_K^{\kappa(i)} a_i(t), \quad t \in \mathbb{Z}_{KW}. \tag{8}$$

Together with Proposition 1, this gives

$$C(\boldsymbol{a}_i;\tau) = \begin{cases} C(\boldsymbol{a}_i;0)\omega_K^{\kappa(i)\tau/W} & \text{for } \tau \in W\mathbb{Z}_{KW} \\ 0 & \text{otherwise.} \end{cases}$$

Let $\boldsymbol{f}_i = \{f_i(t) \mid t \in \mathbb{Z}_K\}$ be defined by $f_i(t) = \omega_K^{\kappa(i)t}$. Then,

$$C(\boldsymbol{a}_i;\cdot) = C(\boldsymbol{a}_i;0)(\mathrm{E}_W \circ \boldsymbol{f}_i). \tag{9}$$

Since DFT $\circ \boldsymbol{f}_i$ is supported only at $K-\kappa(i)$, Known fact 2 gives

$$|(\mathrm{DFT} \circ \boldsymbol{a}_i)(n)| = \begin{cases} \sqrt{C(\boldsymbol{a}_i;0)/W} & \text{for } n+\kappa(i) \in K\mathbb{Z}_{KW} \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

Since the family is uncorrelated, the supports in (10) must be disjoint for different i. Hence

$$\{\kappa(i) \pmod{K} \mid i = 0,1,\ldots,K-1\} = \{0,1,\ldots,K-1\}. \tag{11}$$

Without loss of generality, we may reorder the indices and assume that $\kappa(i) = i$ for $i = 0,1,\ldots,K-1$. Define

$$g_i(t) \triangleq a_i(t)\omega_{KW}^{-it}, \quad t = 0,1,\ldots,W-1. \tag{12}$$

Then, by (8), each $\boldsymbol{a}_i$ can be represented as in (7).

It remains to show that each $\boldsymbol{g}_i = \{g_i(t) \mid t \in \mathbb{Z}_W\}$ is perfect. Applying Known fact 2 to the representation (7), we obtain

$$\begin{aligned}&(\mathrm{DFT} \circ \boldsymbol{a}_i)(n) \\ &= \begin{cases} \sqrt{K}(\mathrm{DFT} \circ \boldsymbol{g}_i)((n+i)/K) & \text{for } n+i \in K\mathbb{Z}_{KW} \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Comparing this with (10), we get

$$|(\mathrm{DFT} \circ \boldsymbol{g}_i)(n)| = \sqrt{\frac{C(\boldsymbol{a}_i;0)}{KW}}, \quad n \in \mathbb{Z}_W.$$

Thus, DFT $\circ\, \boldsymbol{g}_i$ has constant magnitude, and hence $\boldsymbol{g}_i$ is a perfect sequence by Known fact 2. Therefore, $\mathcal{A}$ comes from Popović's construction. ∎

The relations (8) and (11) in the above proof imply the following for the polyphase case:

Corollary 2: Any polyphase uncorrelated optimal (KW,K,W)-ZCZ sequence family must be over an alphabet of size at least K.

V. UNIFIED CONSTRUCTION OF POLYPHASE UNCORRELATED OPTIMAL ZCZ SEQUENCE FAMILIES

Sequence families with good or favourable correlation properties are most useful and practical when they are over the polyphase alphabet [9], [11]. In this case, in particular, it would be better when the alphabet size becomes smaller [9, p. 255]. The best would therefore be the sequences over the polyphase binary alphabet $\{+1,-1\} \subset \mathbb{C}$. From a practical viewpoint, a smaller polyphase alphabet reduces the required phase resolution and implementation complexity, which is relevant when such sequence families are used for synchronization, interference suppression, and waveform design in communication and radar systems. We are now interested in how small the alphabet size could be for an uncorrelated optimal ZCZ sequence family.

In this subsection, we propose a construction of uncorrelated optimal ZCZ sequence families over general polyphase alphabets. We also discuss the alphabet-size consequences of this construction. To keep the statements clear, we distinguish unconditional lower bounds from those that depend on Mow's conjectures. Unconditionally, Corollary 2 gives a lower bound on the alphabet size, which can be tight in some cases and loose in others. A conjectural numerical lower bound is obtained from the following conjecture of Mow:

Conjecture 1 (Mow's Conjecture [20]): Let s be a square-free integer. Then, for any m, a polyphase perfect sequence of length sm^2 exists if and only if its alphabet size is an integer multiple of the following:

$$N_{min}(sm^2) = \begin{cases} 2sm, & \text{: if } s \text{ is even and } m \text{ is odd,} \\ sm, & \text{: otherwise.} \end{cases} \tag{13}$$

Note that interleaving is an alphabet preserving operation. Therefore, we obtain the following conclusion on the alphabet size of the polyphase uncorrelated optimal family of ZCZ sequences using Corollary 1:

Remark 2: The following two statements should be interpreted separately. The first one is unconditional, whereas the second one is conditional on Conjecture 1.

1) Unconditionally, the alphabet size of the polyphase uncorrelated optimal (KW,K,W)-ZCZ sequence family is lower bounded by the minimum alphabet size of the polyphase perfect sequence of length K^2W.
2) Assuming the truth of Conjecture 1, we can make this lower bound explicit. Write $W = sm^2$, where s is square-free. Then
$$K^2W = s(mK)^2, \tag{14}$$
and hence the conjectural lower bound is
$$\begin{aligned}N_{min}(K^2W) &= N_{min}(s(mK)^2) \\ &= \begin{cases} 2smK, & \text{: if } s \text{ is even and } mK \text{ is odd,} \\ smK, & \text{: otherwise.} \end{cases}\end{aligned}$$
Thus, under Conjecture 1, the alphabet size of any polyphase uncorrelated optimal (KW,K,W)-ZCZ sequence family is lower bounded by this value.

Known fact 5: ***(Mow's Construction of the polyphase perfect sequences [21])*** *Construct the set* $\boldsymbol{u} * i | i = 0,1,...,m-1$ *of* m *sequences each of length* sm *for some* s *and* m *where* s *is square-free as follows: for any integer* t,

$$u_i(t) \triangleq \omega_{2s}^{\mu(s)\alpha(i)t^2}\omega_{sm}^{\beta(i)t+\gamma(i)} \tag{15}$$

where $\mu(s)$ *is 1 or 2 according to whether* s *is even or odd, respectively, and three maps* α, β, *and* γ *satisfy the following:*

I. $\mathrm{GCD}(\alpha(i), s) = 1$ *for all i where* $\alpha : \{0, 1, ..., m-1\} \to \{1, 2, ..., s\}$*;*

II. $\{\beta(i) \pmod m | i = 0, 1, ..., m-1\}$ *is a permutation of* $\{0, 1, ..., m-1\}$ *where* $\beta : \{0, 1, ..., m-1\} \to \{0, 1, ..., sm-1\}$ *; and*

III. γ *maps* $\{0, 1, ..., m-1\}$ *into the rationals.*

Now, construct a sequence $\boldsymbol{u}$ *of length* $L = sm^2$ *as follows:*

$$\boldsymbol{u} \triangleq \mathcal{I}(\boldsymbol{u}_0; \boldsymbol{u}_1; \cdots; \boldsymbol{u}_{m-1}). \tag{16}$$

Then, the following hold:

1) *The sequence* $\boldsymbol{u}$ *is perfect.*
2) *The alphabet size of the sequence* $\boldsymbol{u}$ *must be an integer multiple of* $N*\min(L)$ *in* (13)*. For an integer N with* $N_{min}(L)|N$*,* $\boldsymbol{u}$ *has an alphabet size N if and only if* $\frac{\gamma(i)N}{sm}$ *is an integer for all i. In particular, for* $N = N_{min}(L)$*, the construction attains the Mow-minimum alphabet size precisely when*
$$\frac{\gamma(i)N_{min}(L)}{sm} \in \mathbb{Z} \quad \text{for all } i. \tag{17}$$
This condition is automatically satisfied, for example, when $\gamma(i) = 0$ *for all i.*
3) *For an integer N with* $N_{min}(L)|N$*, the number of distinct polyphase perfect sequences of length L over an alphabet of size N constructed by the steps leading to* (16) *is given by*
$$\frac{m!s^{m-1}\phi^m(s)N^{m-1}}{m^2},$$
where $\phi(\cdot)$ *is the Euler's totient function. Here, two sequences are regarded to be distinct if they are either cyclically distinct or not a constant multiple of each other.*

For later use, we also recall Mow's conjecture on the completeness of the above construction. Unlike Conjecture 2, which concerns possible alphabet sizes, the following conjecture concerns whether the construction in **Known fact 5** represents all polyphase perfect sequences.

Conjecture 2: (Mow's Conjecture on the Unified Construction [21]) Any polyphase perfect sequence can be constructed from the construction in **Known fact 5**.

Theorem 2: ***(Construction of the polyphase uncorrelated optimal ZCZ sequence family)*** *Construct a set* $\{\boldsymbol{a}_{i,j} | i = 0, 1, ..., K-1$ *and* $j = 0, 1, ..., m-1\}$ *of mK sequences each of length smK for some s, m, K where s is square-free as follows: for any integer t,*

$$a_{i,j}(t) \triangleq \omega_{2s}^{\mu(s)\alpha_z(i,j)t^2}\omega_{smK}^{(\beta_z(i,j)K+i)t+\gamma_z(i,j)} \tag{18}$$

where $\mu(s)$ *is 1 or 2 according to whether s is even or odd, respectively, and three maps* α_z*,* β_z*, and* γ_z *satisfy the following:*

I. $\mathrm{GCD}(\alpha_z(i,j), s) = 1$ *for all* (i,j) *where* $\alpha_z : \{0, 1, ..., K-1\} \times \{0, 1, ..., m-1\} \to \{1, 2, ..., s\}$*;*

II. for any fixed i, $\{\beta_z(i,j) \pmod m | j = 0, 1, ..., m-1\}$ *is a permutation of* $\{0, 1, ..., m-1\}$ *where* $\beta_z : \{0, 1, ..., K-1\} \times \{0, 1, ..., m-1\} \to \{0, 1, ..., sm-1\}$*;*

III. γ_z *maps* $\{0, 1, ..., K-1\} \times \{0, 1, ..., m-1\}$ *into the rationals.*

Now, construct a set $\mathcal{A}_z = \{\boldsymbol{a}_i | i = 0, 1, ..., K-1\}$ *of K sequences of length* $sm^2K(= KW)$ *as follows:*

$$\boldsymbol{a}_i \triangleq \mathcal{I}(\boldsymbol{a}_{i,0}; \boldsymbol{a}_{i,1}; \cdots; \boldsymbol{a}_{i,m-1}) \quad \text{for } i = 0, 1, ..., K-1. \tag{19}$$

Then, the following hold:

1) *The sequence family* $\mathcal{A}_z$ *is a polyphase uncorrelated optimal family of* (KW, K, W)*-ZCZ sequences.*
2) *The alphabet size of the family* $\mathcal{A}_z$ *must be an integer multiple of* $N_{min}(K^2W)$*. Furthermore, for an integer N with* $N_{min}(K^2W)|N$*, the family* $\mathcal{A}_z$ *has an alphabet size N if and only if* $\frac{\gamma_z(i,j)N}{smK}$ *is an integer for all* (i,j)*.*
3) *For an integer N with* $N_{min}(K^2W)|N$*, the number of distinct families of polyphase uncorrelated optimal* (KW, K, W)*-ZCZ sequences over an alphabet size N constructed by steps leading to* (19) *is given by*
$$\left(\frac{m!s^{m-1}\phi^m(s)N^{m-1}}{m^2}\right)^K \tag{20}$$
where $\phi(\cdot)$ *is the Euler's totient function. Here, two families are regarded to be distinct if a member of one family is distinct from all the members of the other family. Two sequences are regarded to be distinct if they are either cyclically distinct or not a constant multiple of each other.*

We first give a brief outline of the main idea. For each fixed i, we first remove from $\boldsymbol{a}_{i,j}$ the linear modulation depending on i and the phase offset depending on j. The resulting sequences have period sm, and their interleaving gives a sequence $\boldsymbol{g}_i$ of length sm^2. By the conditions on α_z, β_z, and γ_z, this sequence $\boldsymbol{g}_i$ is exactly a perfect sequence obtained from Mow's construction. Thus each $\boldsymbol{a}_i$ can be written in Popović form

$$a_i(t) = g_i(t \pmod{sm^2})\omega_{sm^2K}^{it},$$

which proves that the constructed family is an uncorrelated optimal (KW, K, W)-ZCZ sequence family. The alphabet-size assertion is then proved by separating the construction into the part forced by the quadratic and linear terms and the part controlled by $\gamma_z(i,j)$. The former forces the alphabet size to be a multiple of $N_{min}(K^2W)$, while the latter gives the additional necessary and sufficient condition

$$\frac{\gamma_z(i,j)N}{smK} \in \mathbb{Z} \quad \text{for all } (i,j).$$

Finally, the enumeration formula follows by counting the admissible choices of α_z, β_z, and γ_z, and then quotienting by the equivalences arising from cyclic shifts and constant root-of-unity multiples.

Proof of Theorem 2: The proof is deferred to Appendix A. ∎

Remark 3: According to Theorem 2 in, the construction presented in Theorem 2 must follow the Popović form. In fact, Equation (30) in the proof of Theorem 2 explicitly shows that the construction indeed takes the Popović form.

Corollary 3: In Theorem 2, if we set $\alpha_z(i,j) = 1$, $\beta_z(i,j) = j$ and $\gamma_z(i,j) = 0$ for all i and j, the resulting family $\{\boldsymbol{a}_i | i = 0, 1, ..., K-1\}$ forms the uncorrelated optimal (KW, K, W)-ZCZ sequence family constructed over the polyphase alphabet of size $N_{min}(K^2W)$:

$$a_i(t) \triangleq \omega_{2s}^{(1-\mu(s))q^2} \omega_{smK}^{(Kt+i)q} \quad \text{for} \quad t \in \mathbb{Z}_{KW}, \tag{21}$$

where $q \triangleq \lfloor \frac{t}{m} \rfloor$ is the quotient when t is divided by m. Under Conjecture 1, this alphabet size coincides with the conjectural lower bound in Remark 2.

Remark 4: When $W = 1$ (i.e., $s = 1$ and $m = 1$), the construction in Corollary 3 gives an uncorrelated optimal $(K, K, 1)$-ZCZ sequence family over the polyphase alphabet of size $N_{min}(K^2) = K$. In this special case, this value is the true minimum by Corollary 2, independently of Mow's conjecture.

Example 1: From the construction in Corollary 3, we construct a polyphase uncorrelated optimal $(KW = 12, K = 3, W = 4)$-ZCZ sequence family $\mathcal{A}$ over the alphabet of size $N_{min}(36) = 6$. From the given parameters K and W, note that $s = 1, m = 2$ and $(1-\mu(s)) = 0$ in (21). Then, each sequence in $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \boldsymbol{a}_2\}$ becomes the following. Here, we simply write j for ω_6^j where $0 \le j < 6$.

$$a_i(t) \triangleq \omega_{2s}^{(1-\mu(s))q^2} \omega_{smK}^{(Kt+i)q}$$
$$a_i(t) \triangleq \omega_6^{(3t+i)q}$$

$$\begin{aligned}
\boldsymbol{a}_0 &= (0,0,0,3,\ \ 0,0,0,3,\ \ 0,0,0,3),\\
\boldsymbol{a}_1 &= (0,0,1,4,\ \ 2,2,3,0,\ \ 4,4,5,2),\\
\boldsymbol{a}_2 &= (0,0,2,5,\ \ 4,4,0,3,\ \ 2,2,4,1).
\end{aligned}$$

Under Conjecture 1, this alphabet size is the minimum possible one for this parameter set.

By Corollary 1, $\mathcal{I}(\boldsymbol{a}_0; \boldsymbol{a}_1; \boldsymbol{a}_2)$ is a perfect sequence as shown below:

$$\begin{aligned}
\mathcal{I}(\boldsymbol{a}_0; \boldsymbol{a}_1; \boldsymbol{a}_2) = (&0,0,0,0,0,0\\
&0,1,2,3,4,5\\
&0,2,4,0,2,4\\
&0,3,0,3,0,3\\
&0,4,2,0,4,2\\
&0,5,4,3,2,1).
\end{aligned}$$

In fact, $\mathcal{I}(\boldsymbol{a}_0; \boldsymbol{a}_1; \boldsymbol{a}_2)$ can be derived by reading the 6×6 DFT matrix sequentially from the top row to the bottom row. This happens always when $s = 1$ in our construction.

Remark 5: For the family generated from our construction in Cor 3 with $W = m^2$, its interleaved sequence can be derived from the $Km \times Km$ DFT matrix.

We next discuss when the construction in Theorem 2 can be regarded as a unified construction for all polyphase uncorrelated optimal ZCZ sequence families. Since this question is connected with Mow's unified-construction conjecture, stated as Conjecture 2, the following statements are conditional. We give two such statements: the first uses Conjecture 2 restricted to perfect sequences of length K^2W, while the second uses the same conjectural assertion restricted to perfect sequences of length W.

First, if Conjecture 2 holds for polyphase perfect sequences of length K^2W, then Theorem 2 gives a unified construction of polyphase uncorrelated optimal (KW, K, W)-ZCZ sequence families. The converse implication is not claimed here.

Remark 6: If any polyphase perfect sequence of length K^2W can be constructed from the construction in **Known fact 5** then any polyphase uncorrelated optimal (KW, K, W)-ZCZ sequence family can be constructed from the construction in Theorem 2.

The proof is based on lifting the given ZCZ family to a perfect sequence and then pulling Mow's representation back to the family level. Indeed, by Corollary 1, the interleaving of the K members of an arbitrary polyphase uncorrelated optimal (KW, K, W)-ZCZ sequence family is a perfect sequence of length K^2W. If Conjecture 2 holds for this length, then this perfect sequence has Mow's form. Using Theorem 1, the coefficients in this Mow representation can be grouped according to their residues modulo K, and after a suitable relabeling, they give a triple $(\alpha_z, \beta_z, \gamma_z)$ satisfying the conditions of Theorem 2. Hence the original family is produced by the construction in Theorem 2.

Proof of Remark 6: We write $W = sm^2$, where s is square-free, and assume that every polyphase perfect sequence of length K^2W can be constructed from **Known fact 5**. Let $\mathcal{B} = \{\boldsymbol{b}_i | i = 0, 1, \ldots, K-1\}$ be a polyphase uncorrelated optimal (KW, K, W)-ZCZ sequence family. By Corollary 1,

$$\boldsymbol{u} \triangleq \mathcal{I}(\boldsymbol{b}_0; \boldsymbol{b}_1; \cdots; \boldsymbol{b}_{K-1}) \tag{22}$$

is a polyphase perfect sequence of length $K^2W = s(mK)^2$.

We apply the assumed Mow representation to this interleaved perfect sequence. Then $\boldsymbol{u}$ has the form

$$\boldsymbol{u} = \mathcal{I}(\boldsymbol{u}_0; \boldsymbol{u}_1; \cdots; \boldsymbol{u}_{mK-1}) \quad \text{with} \tag{23}$$

$$u_i(t) = \omega_{smK}^{mK\mu(s)\alpha(i)t^2 + \beta(i)t + \gamma(i)}, \tag{24}$$

for $i \in \{0, 1, \ldots, mK-1\}$ and $t \in \mathbb{Z}_{smK}$, where α, β, and γ satisfy the conditions in **Known fact 5** with m replaced by mK.

Comparing the two interleavings in (22) and (23), we have, for $i \in \{0, 1, \ldots, K-1\}$,

$$\boldsymbol{b}_i = \mathcal{I}(\boldsymbol{u}_i; \boldsymbol{u}_{K+i}; \boldsymbol{u}_{2K+i}; \cdots; \boldsymbol{u}_{(m-1)K+i}). \tag{25}$$

Let $\boldsymbol{u}_{i,j} \triangleq \boldsymbol{u}_{jK+i}$ for

$$(i,j) \in \{0, 1, \ldots, K-1\} \times \{0, 1, \ldots, m-1\}.$$

By Theorem 1, there exists a permutation κ of $\{0, 1, \ldots, K -$

$1\}$ such that

$$\frac{b_i(t+sm^2)}{b_i(t)}=\omega_K^{\kappa(i)}$$

for $i\in\{0,1,\dots,K-1\}$ and $t\in\mathbb{Z}_{sm^2}$. Therefore, by (25),

$$\frac{u_{i,j}(t+sm)}{u_{i,j}(t)}=\omega_K^{\kappa(i)}$$

for $(i,j)\in\{0,1,\dots,K-1\}\times\{0,1,\dots,m-1\}$ and $t\in\mathbb{Z}_{sm}$. On the other hand, from (24),

$$\frac{u_{i,j}(t+sm)}{u_{i,j}(t)}=\omega_K^{\beta(jK+i)}.$$

Hence

$$\beta(jK+i)\equiv\kappa(i)\pmod{K}.$$

This congruence is the key step that converts the Mow parameters into the parameters required in Theorem 2. Since $\{\beta(\ell)\pmod{mK}|\ell=0,1,\dots,mK-1\}$ is a permutation of $\{0,1,\dots,mK-1\}$, it follows that, for each fixed i,

$$\left\{\frac{\beta(jK+i)-\kappa(i)}{K}\pmod{m}\,\middle|\,j=0,1,\dots,m-1\right\}$$
$$=\{0,1,\dots,m-1\}.$$

Now define

$$\alpha_z(\kappa(i),j)\triangleq\alpha(jK+i),$$
$$\beta_z(\kappa(i),j)\triangleq\frac{\beta(jK+i)-\kappa(i)}{K},$$
$$\gamma_z(\kappa(i),j)\triangleq\gamma(jK+i),$$

and set $\boldsymbol{a}_{\kappa(i)}\triangleq\boldsymbol{b}_i$. Then α_z satisfies Condition I of Theorem 2, the above permutation property gives Condition II, and γ_z satisfies Condition III. Consequently, the triple $(\alpha_z,\beta_z,\gamma_z)$ satisfies all the conditions in Theorem 2, and

$$\mathcal{B}=\{\boldsymbol{a}_i|i=0,1,\dots,K-1\}$$

can be constructed from (19). ■

We now give a length-W version of the preceding conditional statement. In this case, the connection with Conjecture 2 becomes an equivalence.

Remark 7: The following two statements are equivalent:

1) Every polyphase perfect sequence of length W can be constructed from the construction in **Known fact 5**.
2) Every polyphase uncorrelated optimal (KW,K,W)-ZCZ sequence family can be constructed from the construction in Theorem 2.

Proof of Remark 7: We write $W=sm^2$, where s is square-free.

1) implies 2): Assume that every polyphase perfect sequence of length W can be constructed from the construction in **Known fact 5**. Let $\mathcal{B}=\{\boldsymbol{b}_i|i=0,1,\dots,K-1\}$ be a polyphase uncorrelated optimal (KW,K,W)-ZCZ sequence family. By Theorem 1, each member of $\mathcal{B}$ has the Popović form

$$b_i(t)=g_i(t\pmod{sm^2})\omega_{sm^2K}^{it}\quad\text{for }t\in\mathbb{Z}_{sm^2K},\tag{26}$$

where $\boldsymbol{g}_i$ is a polyphase perfect sequence of length sm^2.

By the assumption, each $\boldsymbol{g}_i$ can be constructed from **Known fact 5**. Thus, for each i, we may write

$$\boldsymbol{g}_i=\mathcal{I}(\boldsymbol{g}_{i,0};\boldsymbol{g}_{i,1};\cdots;\boldsymbol{g}_{i,m-1}),$$

where

$$g_{i,j}(t)=\omega_{2s}^{\mu(s)\alpha_i(j)t^2}\omega_{sm}^{\beta_i(j)t+\gamma_i(j)}\quad\text{for }t\in\mathbb{Z}_{sm}.$$

Here, for each fixed i, the maps α_i, β_i, and γ_i satisfy the conditions in **Known fact 5**.

Define sequences $\boldsymbol{b}_{i,j}$ of length smK by

$$b_{i,j}(t)\triangleq g_{i,j}(t\pmod{sm})\omega_{smK}^{it}\omega_{sm^2K}^{j}\quad\text{for }t\in\mathbb{Z}_{smK}.$$

Then

$$\boldsymbol{b}_i=\mathcal{I}(\boldsymbol{b}_{i,0};\boldsymbol{b}_{i,1};\cdots;\boldsymbol{b}_{i,m-1})$$

and

$$b_{i,j}(t)=\omega_{2s}^{\mu(s)\alpha_i(j)t^2}\omega_{smK}^{(\beta_i(j)K+i)t+\gamma_i(j)K+j/m}.$$

Therefore, by setting

$$\alpha_z(i,j)\triangleq\alpha_i(j),\quad\beta_z(i,j)\triangleq\beta_i(j),\quad\gamma_z(i,j)\triangleq\gamma_i(j)K+\frac{j}{m},$$

the sequences $\boldsymbol{b}_{i,j}$ have exactly the form in (18). Moreover, the conditions on α_z, β_z, and γ_z in Theorem 2 follow directly from the corresponding conditions on α_i, β_i, and γ_i in **Known fact 5**. Hence $\mathcal{B}$ can be constructed from Theorem 2.

2) implies 1): Assume that every polyphase uncorrelated optimal (KW,K,W)-ZCZ sequence family can be constructed from Theorem 2. Let $\boldsymbol{g}$ be an arbitrary polyphase perfect sequence of length W. By Popović's construction, the family $\mathcal{B}=\{\boldsymbol{b}_i|i=0,1,\dots,K-1\}$ defined by

$$b_i(t)=g(t\pmod{W})\omega_{KW}^{it}\quad\text{for }t\in\mathbb{Z}_{KW}$$

is a polyphase uncorrelated optimal (KW,K,W)-ZCZ sequence family.

By the assumption, $\mathcal{B}$ can be constructed from Theorem 2. However, in the proof of the first item of Theorem 2, every family constructed from Theorem 2 is shown to have the Popović form with base perfect sequences obtained from **Known fact 5**. Therefore, the perfect sequence $\boldsymbol{g}$ can be constructed from **Known fact 5**. Since $\boldsymbol{g}$ was arbitrary, every polyphase perfect sequence of length W can be constructed from **Known fact 5**. ■

VI. A CONVERSE TO COROLLARY 1 AND SOME CONCLUDING REMARKS

A. A CONVERSE TO COROLLARY 1

Given a sequence family $\boldsymbol{a}_0,\boldsymbol{a}_1,\dots,\boldsymbol{a}_{K-1}$ all of length KW, its interleaved sequence is denoted by

$$\boldsymbol{a}=\mathcal{I}(\boldsymbol{a}_0;\boldsymbol{a}_1;\cdots;\boldsymbol{a}_{K-1}).$$

Conversely, given a sequence $\boldsymbol{b}$ of length K^2W, we may deinterleave this to obtain a family of K sequences all of length KW. Here, we write $\boldsymbol{b}$ in an array of size $KW\times K$ row by row and the K sequences are just the column sequences. Specifically, this can be represented as follows. Using the notation $\boldsymbol{b} = \{b(t)|t = 0, 1, ..., K^2W - 1\}$, we have a deinterleaved family $\boldsymbol{b}_0, \boldsymbol{b}_1, ..., \boldsymbol{b}_{K-1}$ where $\boldsymbol{b}_i = b_i(t)|t = 0, 1, ..., KW - 1$ where

$$b_i(t) = b(tK + i) \quad \text{for } t = 0, 1, ..., KW - 1$$

for each $i = 0, 1, ..., K - 1$. The deinterleaved family of sequences from $\boldsymbol{b}$ is denoted by

$$\mathcal{DI}_K(\boldsymbol{b}) = \boldsymbol{b}_0, \boldsymbol{b}_1, ..., \boldsymbol{b}_{K-1},$$

where each $\boldsymbol{b}_i$ has length KW.

Corollary 1 says that interleaving all the sequences in any polyphase uncorrelated optimal (KW, K, W)-ZCZ sequence family yields a polyphase perfect sequence of length K^2W. We are now interested in its converse. That is, we would like to have a polyphase uncorrelated optimal (KW, K, W)-ZCZ sequence family by deinterleaving a given polyphase perfect sequence of length K^2W. In this section, we focus mainly on the case $W = 1$, where the converse question is most closely related to perfect sequences of square length.

Conjecture 3: For any polyphase perfect sequence $\boldsymbol{a}$ of length K^2, the deinterleaved family $\mathcal{DI}_K(\boldsymbol{a})$ is an uncorrelated optimal $(K, K, 1)$-ZCZ sequence family.

Conjecture 3 should be regarded as a conjectural converse to Corollary 1. It is not used in the proofs of the main results of this paper.

A Fermat-quotient sequence is a recently discovered polyphase perfect sequence of length p^2 for any odd prime p [23], [24]. We are able to confirm the above conjecture to be true for Fermat-quotient sequences. To explain this, we recall the definition of Fermat-quotient sequences. For an odd prime integer p, the Fermat-quotient sequence $\boldsymbol{f} = f(t)|t \in \mathbb{Z} * p^2$ of length p^2 is defined by [23], [24]

$$f(t) = \omega_p^{F(t)} \quad \text{for } t \in \mathbb{Z} * p^2,$$

where

$$F(t) \triangleq \begin{cases} \frac{t^{p-1}-1}{p} \pmod p & \text{if} \quad t \in \mathbb{Z} * p^2 \backslash p\mathbb{Z} * p^2 \\ 0 & \text{if} \quad t \in p\mathbb{Z}_{p^2}. \end{cases}$$

Proposition 4: Let $\boldsymbol{f} = f(t)|t \in \mathbb{Z}_{p^2}$ be a Fermat-quotient sequence of length p^2. Then, $\mathcal{DI}_p(\boldsymbol{f})$ is an uncorrelated optimal $(p, p, 1)$-ZCZ sequence family.

Proof: Let $\mathcal{DI}_p(\boldsymbol{f}) = \boldsymbol{f}_0, \boldsymbol{f} * 1, ..., \boldsymbol{f} * p - 1$ where $\boldsymbol{f} = \mathcal{I}(\boldsymbol{f}_0; \boldsymbol{f}*1; \cdots; \boldsymbol{f}*p-1)$. By definition and from [24, Lemma 1, item 3], for any integer t, we have

$$f_i(t) = f(pt + i) = f(i)\omega_p^{P(i)t},$$

where $P(i) \triangleq -i^{-1} \pmod p$ for $i \neq 0$ and $P(0) = 0$. Note that the i-th term $f(i)$ of $\boldsymbol{f}$ is a perfect sequence of length 1 and $P(\cdot)$ is a permutation of $\mathbb{Z}_p$. Therefore, the deinterleaved family $\mathcal{DI}_p(\boldsymbol{f})$ must be an uncorrelated optimal $(p, p, 1)$-ZCZ sequence family by Popović's construction in **Known fact 4**. ■

In fact, Mow's unified construction for perfect sequences of length K^2 is nothing but the interleaved sequence of an uncorrelated optimal family of $(K, K, 1)$-ZCZ sequences [21]. Therefore, we see that, for any polyphase perfect sequence $\boldsymbol{a}$ of length K^2 constructed from Mow's unified construction in [21], its deinterleaved family $\mathcal{DI}_K(\boldsymbol{a})$ is an uncorrelated optimal family of $(K, K, 1)$-ZCZ sequences. We note that to the best of our knowledge, all the known polyphase perfect sequences so far, including complex Fermat-quotient sequences, can be constructed using Mow's unified construction [21], [30].

The deinterleaved family from a polyphase perfect sequence of length WK^2, for $W > 1$, will not always be an optimal uncorrelated ZCZ sequence family.

Example 2: Consider an uncorrelated optimal family of $(4, 4, 1)$-ZCZ sequences:

$$\begin{aligned} \boldsymbol{b}_0 &= (+1, +1, +1, +1), \\ \boldsymbol{b}_1 &= (+1, -1, +1, -1), \\ \boldsymbol{b}_2 &= (+1, +j, -1, -j), \\ \boldsymbol{b}_3 &= (+1, -j, -1, +j), \end{aligned}$$

which are 4 rows of the 4×4 DFT matrix (see Remark 5), where $j \triangleq \sqrt{-1}$. The interleaved sequence of this family becomes a polyphase perfect sequence of length 16 given by

$$\begin{aligned} \boldsymbol{b} \triangleq (&+1, +1, +1, +1, \quad +1, -1, +j, -j, \\ &+1, +1, -1, -1, \quad +1, -1, -j, +j). \end{aligned}$$

Using $K = 4$ and $W = 1$, the deinterleaved family from $\boldsymbol{b}$ becomes the original $\boldsymbol{b}_i$'s with which we have started, trivially. On the other hand, using $K = 2$ and $W = 4$, we have the deinterleaved family $\boldsymbol{a}_0, \boldsymbol{a}_1$ given by

$$\begin{aligned} \mathcal{DI}_2(\boldsymbol{b}) = \{&\boldsymbol{a}_0 \triangleq (+1, +1, +1, +j, +1, -1, +1, -j), \\ &\boldsymbol{a}_1 \triangleq (+1, +1, -1, -j, +1, -1, -1, +j)\}, \end{aligned}$$

which is not an $(8, 2, 4)$-ZCZ sequence family since ZCZ width is smaller than 4, and hence, it is not an optimal family.

On the other hand, it is interesting to see that the family $\mathcal{DI}_2(\boldsymbol{b})$ is an uncorrelated sequence family.

If Conjecture 3 is true, then, by Corollary 2, there cannot exist a polyphase perfect sequence of length K^2 over an alphabet of size less than K. The case of even $K > 2$ corresponds to the circulant Hadamard conjecture.

Remark 8: If Conjecture 3 is true, then the circulant Hadamard conjecture is true.

B. CONCLUDING REMARKS

In summary, this paper provides the following key results: Theorem 1 proves that any uncorrelated optimal ZCZ sequence family comes from Popović's construction. Theorem 2 proposes a unified construction for polyphase uncorrelated optimal ZCZ sequence families. Remarks 6 and 7 show that any polyphase perfect sequence comes from Mow's unified construction if and only if any polyphase uncorrelated optimal ZCZ sequence family comes from Theorem 2.

The alphabet-size result should also be interpreted under the assumptions stated in Corollary 2. In particular, the lower bound on the alphabet size is obtained for polyphase uncorrelated optimal ZCZ sequence families satisfying the hypotheses of that corollary. Thus, the result is not intended as a lower bound for arbitrary ZCZ sequence families outside the optimal uncorrelated setting considered in this paper.

Additionally, we prove that interleaving sequences from an uncorrelated optimal ZCZ sequence family always produces a perfect sequence. While the converse, deinterleaving a perfect sequence of length K^2 yielding an uncorrelated optimal (K, K, 1)-ZCZ sequence family, remains unproven, we confirm it for all known polyphase perfect sequences, including Fermat-quotient sequences. This conjectural converse, if true, would provide further evidence supporting the nonexistence of certain perfect sequences with small alphabet size.

From a practical viewpoint, the results of this paper are relevant to the design of sequence families for systems requiring low interference under limited timing uncertainty. ZCZ sequence families are useful in quasi-synchronous multiuser communication, synchronization, radar, sonar, and integrated sensing and communication systems, where correlation sidelobes inside a prescribed delay zone should be suppressed. The uncorrelated optimal families studied here are especially desirable because they achieve the maximum possible family size for the given sequence length and ZCZ width. The structural theorem shows that every such optimal family must have Popović's form, thereby narrowing the design space and providing a systematic way to search for or construct sequence families with prescribed alphabet and correlation properties. The interleaving connection with perfect sequences also provides a bridge between perfect-sequence design and ZCZ-family design, which may be useful in applications where both low autocorrelation and controlled multiuser interference are required.

APPENDIX A PROOF OF THEOREM 2

Proof of 1): For each pair $(i,j) \in \{0,1,...,K-1\} \times \{0,1,...,m-1\}$, let $\boldsymbol{a}'_{i,j}$ be a sequence of length smK given by

$$a'_{i,j}(t) \triangleq a_{i,j}(t)\omega_{smK}^{-it}\omega_{sm^2K}^{-j} \quad \text{for } t \in \mathbb{Z}_{smK}. \tag{27}$$

Then, from (18), for $t \in \mathbb{Z}_{smK}$,

$$a'_{i,j}(t) = \omega_{2s}^{\mu(s)\alpha_z(i,j)t^2}\omega_{sm}^{\beta_z(i,j)t}\omega_{sm^2K}^{-j+m\gamma_z(i,j)}. \tag{28}$$

Observe that the above has the period sm. Let $\boldsymbol{a}''_{i,j}$ be a sequence of length sm given by $a''_{i,j}(t) \triangleq a'_{i,j}(t)$ for $t \in \mathbb{Z}_{sm}$ and consider the interleaved sequence

$$\boldsymbol{g}_i \triangleq \mathcal{I}(\boldsymbol{a}''_{i,0};\boldsymbol{a}''_{i,1};\cdots;\boldsymbol{a}''_{i,m-1}) \tag{29}$$

of length sm^2. Then, by definition of interleaved sequence and from (27) and (19),

$$a_i(t) = g_i(t \pmod{sm^2})\omega_{sm^2K}^{it} \quad \text{for } t \in \mathbb{Z}_{sm^2K}. \tag{30}$$

Now, it is sufficient to show that $\boldsymbol{g}_i$ is a perfect sequence. From (28) and the definition of $\boldsymbol{a}''_{i,j}$, for $t \in \mathbb{Z}_{sm}$,

$$a''_{i,j}(t) = \omega_{2s}^{\mu(s)\alpha_z(i,j)t^2}\omega_{sm}^{\beta_z(i,j)t+\frac{-j+m\gamma_z(i,j)}{mK}}.$$

Therefore, for a fixed $i \in \{0,1,...,K-1\}$, $\boldsymbol{a}_j$ in (15) is the same as above where $\alpha(j) \triangleq \alpha_z(i,j)$, $\beta(j) \triangleq \beta_z(i,j)$ and $\gamma(j) \triangleq \frac{-j+m\gamma_z(i,j)}{mK}$. The conditions I, II and III of **Known fact 5** for these α, β and γ are implied by the conditions I, II and III of this theorem for α_z, β_z and γ_z. Therefore $\boldsymbol{g}_i$ in (29) is a perfect sequence which comes from Mow's unified construction as in (16) of **Known fact 5**.

Proof of 2): First, we show that the alphabet size of $\mathcal{A}_z$ must be an integer multiple of $N_{min}(K^2W)$. For $K \leq 2$, the proof is straightforward and is omitted here for brevity. We assume $K > 2$.

Let

$$M \triangleq mK, \qquad d \triangleq \mathrm{GCD}(s,M),$$

and let s_1 and M_1 be positive integers satisfying

$$s = s_1 d, \qquad M = M_1 d.$$

Put

$$R \triangleq N_{min}(K^2W).$$

Since every element of a polyphase alphabet of size N is an integer power of ω_N, the ratio of any two elements in the alphabet is also an integer power of ω_N. Hence, if there exist two entries in $\mathcal{A}_z$ whose ratio has exact order R, then R must divide N.

By Condition II, there exist $j_1, j_2 \in \{0,1,\ldots,m-1\}$ such that

$$\beta_z(1,j_1) = q_1 m, \qquad \beta_z(2,j_2) = q_2 m$$

for some integers q_1 and q_2. Let

$$\alpha_1 \triangleq \alpha_z(1,j_1), \qquad \alpha_2 \triangleq \alpha_z(2,j_2).$$

From (18), we have

$$\frac{a_{1,j_1}(t+1)}{a_{1,j_1}(t)} = \omega_{2s}^{\mu(s)\alpha_1(2t+1)}\omega_{sM}^{q_1M+1} \tag{31}$$

and

$$\frac{a_{2,j_2}(t+1)}{a_{2,j_2}(t)} = \omega_{2s}^{\mu(s)\alpha_2(2t+1)}\omega_{sM}^{q_2M+2}. \tag{32}$$

It remains to show that, for some t, one of the two ratios in (31) and (32) has exact order R.

We use the following elementary fact: if $\xi = \omega_R^E$ and $\mathrm{GCD}(E,R) = 1$, then ξ has exact order R.

We divide the proof into three cases.

- *The case where s is odd.* In this case, $\mu(s) = 2$ and

$$R = sM = s_1 M_1 d^2.$$

Then (31) becomes

$$\frac{a_{1,j_1}(t+1)}{a_{1,j_1}(t)} = \omega_R^{(\alpha_1(2t+1)+q_1)M_1 d+1}. \tag{33}$$

Since $\mathrm{GCD}(\alpha_1, s_1) = 1$ and s_1 is odd, there exists an integer t such that

$$s_1 \mid \alpha_1(2t+1) + q_1.$$

For this value of t, the exponent in (33) is congruent to 1 modulo s_1, M_1, and d. Hence it is relatively prime to $s_1 M_1 d^2 = R$. Therefore, the ratio in (33) has exact order R.

- *The case where s is even and M is odd.* In this case, $\mu(s) = 1$, d and M_1 are odd, $s_1/2$ is odd, and

$$R = 2sM = 2s_1 M_1 d^2.$$

Then (31) becomes

$$\frac{a_{1,j_1}(t+1)}{a_{1,j_1}(t)} = \omega_R^{(\alpha_1(2t+1)+2q_1)M_1 d+2}. \tag{34}$$

Since $\mathrm{GCD}(\alpha_1, s_1/2) = 1$ and $s_1/2$ is odd, there exists an integer t such that

$$\frac{s_1}{2} \mid \alpha_1(2t+1) + 2q_1.$$

For this value of t, the exponent in (34) is congruent to 2 modulo $s_1/2$, M_1, and d. Since $s_1/2$, M_1, and d are odd, this exponent is relatively prime to each of them. Also, the exponent is odd because α_1, $2t+1$, M_1, and d are odd. Thus the exponent is relatively prime to $2s_1M_1d^2 = R$. Therefore, the ratio in (34) has exact order R.

- *The case where both s and M are even.* In this case, $\mu(s) = 1$, s_1 is odd, d is even, $d/2$ is odd, and

$$R = sM = s_1 M_1 d^2.$$

Equations (31) and (32) become

$$\frac{a_{1,j_1}(t+1)}{a_{1,j_1}(t)} = \omega_R^{(\alpha_1(2t+1)+2q_1)M_1(d/2)+1} \tag{35}$$

and

$$\frac{a_{2,j_2}(t+1)}{a_{2,j_2}(t)} = \omega_R^{(\alpha_2(2t+1)+2q_2)M_1(d/2)+2}. \tag{36}$$

Since $\mathrm{GCD}(\alpha_1, s_1) = \mathrm{GCD}(\alpha_2, s_1) = 1$ and s_1 is odd, there exist integers t_1 and t_2 such that

$$s_1 \mid \alpha_1(2t_1+1) + 2q_1$$

and

$$s_1 \mid \alpha_2(2t_2+1) + 2q_2.$$

If M_1 is even, then we use (35) with $t = t_1$. The exponent is congruent to 1 modulo s_1, M_1, and $d/2$. Also, it is odd. Hence it is relatively prime to $s_1 M_1 d^2 = R$.
If M_1 is odd, then we use (36) with $t = t_2$. The exponent is congruent to 2 modulo s_1, M_1, and $d/2$. Since s_1, M_1, and $d/2$ are odd, it is relatively prime to each of them. Also, it is odd. Hence it is relatively prime to $s_1 M_1 d^2 = R$.
Therefore, in all cases, there exists a ratio of two entries of $\mathcal{A}_z$ having exact order $R = N_{min}(K^2W)$. Hence the alphabet size of $\mathcal{A}_z$ must be an integer multiple of $N_{min}(K^2W)$.

We now prove the remaining assertion. Let N be an integer satisfying

$$N_{min}(K^2W) \mid N.$$

We show that $\mathcal{A}_z$ has alphabet size N if and only if

$$\frac{\gamma_z(i,j)N}{smK}$$

is an integer for all (i,j).

For each (i,j), the right-hand side of (18) can be decomposed as

$$a_{i,j}(t) = \left(\omega_{2s}^{\mu(s)\alpha_z(i,j)t^2}\,\omega_{smK}^{(\beta_z(i,j)K+i)t}\right)\omega_{smK}^{\gamma_z(i,j)}. \tag{37}$$

The first factor in (37) is always an integer power of $\omega_{N_{min}(K^2W)}$. Indeed, if s is odd, then $\mu(s) = 2$ and the first factor is an integer power of

$$\omega_{\mathrm{LCM}(s,smK)} = \omega_{N_{min}(K^2W)}.$$

If s is even, then $\mu(s) = 1$ and the first factor is an integer power of

$$\omega_{\mathrm{LCM}(2s,smK)} = \omega_{N_{min}(K^2W)}.$$

Since $N_{min}(K^2W) \mid N$, the first factor in (37) is also an integer power of ω_N.

Therefore, all entries $a_{i,j}(t)$ are integer powers of ω_N if and only if

$$\omega_{smK}^{\gamma_z(i,j)}$$

is an integer power of ω_N for every (i,j). This is equivalent to

$$\frac{\gamma_z(i,j)N}{smK} \in \mathbb{Z}$$

for every (i,j).

For necessity, one may also take $t = 0$ in (37). Then

$$a_{i,j}(0) = \omega_{smK}^{\gamma_z(i,j)},$$

so $\omega_{smK}^{\gamma_z(i,j)}$ must itself be an integer power of ω_N. Hence

$$\frac{\gamma_z(i,j)N}{smK} \in \mathbb{Z}$$

is necessary. The sufficiency follows from the preceding paragraph.

Proof of 3): In this proof, we consider various senses of family distinctness and equivalence. To avoid ambiguity, we define the following terms:

- Two families are considered *strict-sense equivalent* if, in their original form, every member of one family is identical to some member of the other family. If two families are not strict-sense equivalent, we consider them to be *strict-sense distinct*.
- Two families are considered *equivalent under cyclic shift* if, for every member of one family, there exists a cyclic shift of this member identical to some member of the other family. If two families are not equivalent under cyclic shift, we consider them to be *distinct under cyclic shift*.

- Two families are considered *equivalent under constant root-of-unity multiple* if, for every member of one family, there exists a constant root-of-unity multiple of this member identical to some member of the other family. If two families are not equivalent under constant multiple, we consider them to be *distinct under constant root-of-unity multiple*.
- Two families are considered *universally equivalent* if, for every member of one family, there exists a combination of cyclic shift and constant root-of-unity multiple of this member that is identical to some member of the other family. If two families are not universally equivalent, we consider them to be *universally distinct*.

Since replacing $\gamma_z(i,j)$ with $\gamma_z(i,j)+smK$ does not change (18), we assume that $0 \le \gamma_z(i,j) < smK$ for all i,j. Under this assumption, it is obvious that distinct function triples for $(\alpha_z,\beta_z,\gamma_z)$ generate *strict-sense distinct* families for $\mathcal{A}_z$. Therefore, we will first count the number of function triples for $(\alpha_z,\beta_z,\gamma_z)$ that satisfy the condition I, II and III, and then remove duplicates caused by cyclic shifts and constant multiplication to obtain the final count for *universally distinct* families.

For each pair $(i,j) \in \{0,1,\ldots,K-1\}\times\{0,1,\ldots,m-1\}$, the number of values for $\alpha_z(i,j)$ satisfying $\mathrm{GCD}(\alpha_z(i,j),s)=1$ and $0 \le \alpha_z(i,j) < s$ is $\phi(s)$. Therefore, the number of all the functions for α_z satisfying the condition I is

$$\phi(s)^{mK}. \tag{38}$$

For each pair $(i,j) \in \{0,1,\ldots,K-1\}\times\{0,1,\ldots,m-1\}$, let $q_{i,j}$ and $r_{i,j}$ be the quotient and the remainder when $\beta_z(i,j)$ is divided by m, respectively. According to the condition II, for all (i,j), $q_{i,j}$ is a non-negative integer less than s, and for a fixed $i \in \{0,1,\ldots,K-1\}$, $\{r_{i,j}|j=0,1,\ldots,m-1\}$ is a permutation of $\{0,1,\ldots,m-1\}$. Therefore, the number of all the functions for β_z satisfying the condition II is

$$s^{mK}(m!)^K. \tag{39}$$

For each pair $(i,j) \in \{0,1,\ldots,K-1\}\times\{0,1,\ldots,m-1\}$, by the second item of this theorem and our assumption of $0 \le \gamma_z(i,j) < smK$, $\gamma_z(i,j)$ must be chosen from the following N values:

$$\gamma_z(i,j) = 0, \frac{smK}{N}, \frac{2smK}{N}, \ldots, \frac{(N-1)smK}{N}.$$

Therefore, the number of all the possible functions for γ_z is

$$N^{mK}. \tag{40}$$

Since the condition I for α_z, the condition II for β_z and the condition III for γ_z are independent of each other, the number of possible function triples for $(\alpha_z,\beta_z,\gamma_z)$ is the product of (38), (39) and (40) as follows:

$$\phi(s)^{mK}s^{mK}(m!)^K N^{mK}. \tag{41}$$

We will now remove duplicates caused by cyclic shifts and constant multiplication from the above. To do so, we use the following two lemmas.

Lemma 1: Consider a family $\mathcal{A}_z$ constructed by steps leading to (19). *Then, any* strict-sense equivalent *family of $\mathcal{A}_z$ can also be constructed by steps leading to* (19).

Its proof is given in Appendix B.

Lemma 2: Consider an uncorrelated optimal (KW,K,W)-ZCZ sequence family $\mathcal{B}=\{\boldsymbol{b}_i|i=0,1,\ldots,K-1\}$.

1) *Any family of sequences* universally equivalent *to $\mathcal{B}$ can be constructed by applying an appropriate left cyclic shift by 0 to $W-1$ and a constant root of unity multiple to each sequence in $\mathcal{B}$, with the shifts and multiples potentially varying for each sequence.*
2) *Two families, each constructed by applying left cyclic shifts (within the range 0 to $W-1$) and constant root of unity multiples to sequences in $\mathcal{B}$, with shifts and multiples potentially varying for each sequence, are* strict-sense distinct *if at least one or more sequences in $\mathcal{B}$ are assigned different shifts or multiples between the two families.*

Its proof is given in Appendix C. By Lemma 1, all the families that can be constructed by steps leading to (19) using function triples for $(\alpha_z,\beta_z,\gamma_z)$ satisfying Conditions I, II, and III include all their *universally equivalent* families. Therefore, the number of *universally distinct* families constructed by steps leading to (19) can be obtained by dividing the number of *strict-sense distinct* families obtained in (41) by the number of *universally equivalent* families of a single family. By Lemma 2 a), the number of equivalent families can be determined by considering the left cyclic shift by 0 to $W-1$ and the constant root of unity multiples, where the constant is restricted to integer powers of ω_N to preserve the alphabet size N. From the principle of Lemma 2, this number is WN for each sequence, and thus extends to $(WN)^K$ for each family. Therefore, the desired answer is obtained by dividing (41) by $(WN)^K$, as in (20).

APPENDIX B PROOF OF LEMMA 1

It is sufficient to prove the following two statements:

a) Any sequence family *equivalent* to $\mathcal{A}_z$ *under cyclic shift* can also be constructed by steps leading to (19).
b) Any sequence family *equivalent* to $\mathcal{A}_z$ *under constant root-of-unity multiple* can also be constructed by steps leading to (19).

Proof of a): It is sufficient to show that a family where any single sequence in $\mathcal{A}_z$ is cyclically left shifted by 1 can also be constructed from (19) using another function triple that satisfies the conditions I, II and III. Let $\boldsymbol{a}_{i_1}$ for some integer $i_1 \in \{0,1,\ldots,K-1\}$ be that single sequence. Define $\alpha'_z : \{0,1,\ldots,K-1\}\times\{0,1,\ldots,m-1\}\to\{0,1,\ldots,s-1\}$, $\beta'_z : \{0,1,\ldots,K-1\}\times\{0,1,\ldots,m-1\}\to\{0,1,\ldots,sm-1\}$ and $\gamma'_z : \{0,1,\ldots,K-1\}\times\{0,1,\ldots,m-1\}\to\mathbb{Q}$ as following:

$$\alpha'_z(i,j) \triangleq \begin{cases} \alpha_z(i,j), & \text{for } i \neq i_1 \text{ and all } j, \\ \alpha_z(i_1, j+1), & \text{for } i = i_1 \text{ and } j < m-1, \\ \alpha_z(i_1, 0), & \text{for } i = i_1 \text{ and } j = m-1, \end{cases}$$

$$\beta'_z(i,j) \triangleq \begin{cases} \beta_z(i,j), & \text{for } i \neq i_1 \text{ and all } j, \\ \beta_z(i_1, j+1), & \text{for } i = i_1 \text{ and } j < m-1, \\ \tilde{\beta}_z, & \text{for } i = i_1 \text{ and } j = m-1, \end{cases}$$

where

$$\tilde{\beta}_z \triangleq (\beta_z(i_1,0) + m\mu(s)\alpha_z(i_1,0) \pmod{sm}), \quad \text{and}$$

$$\gamma'_z(i,j) \triangleq \begin{cases} \gamma_z(i,j), & \text{for } i \neq i_1 \text{ and all } j, \\ \gamma_z(i_1, j+1), & \text{for } i = i_1 \text{ and } j < m-1, \\ \tilde{\gamma}_z, & \text{for } i = i_1 \text{ and } j = m-1, \end{cases}$$

where

$$\tilde{\gamma}_z \triangleq \gamma_z(i_1,0) + \beta_z(i_1,0)K + i_1 + \mu(s)\alpha_z(i_1,0)mK/2.$$

The function triple $(\alpha'_z, \beta'_z, \gamma'_z)$ satisfies the conditions I, II and III. Verification is omitted here for simplicity. Constructing a family from (19) using α'_z, β'_z and γ'_z results in a family where only $\boldsymbol{a}_{i_1}$ is cyclically left shifted by 1. It is straightforward to verify but is also omitted for simplicity.

Proof of b): It is sufficient to show that a family where any one sequence in $\mathcal{A}_z$ is multiplied by an arbitrary constant root of unity can also be constructed from (19) using another function triple that satisfies the conditions I, II and III. Let $\boldsymbol{a}_{i_2}$ for some integer $i_2 \in \{0, 1, ..., K-1\}$ be that one sequence and ω_x^y for some integer x and y be that constant root of unity. Define $\gamma''_z : \{0, 1, ..., K-1\} \times \{0, 1, ..., m-1\} \to \mathbb{Q}$ as following:

$$\gamma''_z(i,j) = \begin{cases} \gamma_z(i,j) & \text{for } i \neq i_2 \text{ and all } j, \\ \gamma_z(i_2,j) + \frac{smKy}{x} & \text{for } i = i_2 \text{ and all } j. \end{cases}$$

A family constructed from (19) using α_z, β_z and γ''_z corresponds to the family where only $\boldsymbol{a}_{i_2}$ is multiplied by the constant root of unity ω_x^y. ∎

APPENDIX C PROOF OF LEMMA 2

Since $\mathcal{B}$ is an uncorrelated optimal (KW, K, W)-ZCZ sequence family, the sequence indices can be appropriately rearranged without loss of generality, and by Theorem 1, $\boldsymbol{b}_i$ for $i = 0, 1, ..., K-1$ can be represented as follows.

$$b_i(t) = g_i(t \pmod W)\omega_{KW}^{it} \text{for } t \in \mathbb{Z}_{KW}, \tag{42}$$

for some perfect sequence $\boldsymbol{g}_i$ of length W.

a) It is sufficient to show that for any $\boldsymbol{b}_i \in \mathcal{B}$, $\omega_x^y(T^n \circ \boldsymbol{b}_i)$ for any integers x, y and n can be represented as

$$\omega_x^y(T^n \circ \boldsymbol{b}_i) = \omega_{x'}^{y'}(T^{n'} \circ \boldsymbol{b}_i) \tag{43}$$

for some integers x', y' and n' with $0 \leq n' < W$. LHS of the above at time $t \in \mathbb{Z}_{KW}$ becomes

$$\omega_x^y(T^n \circ \boldsymbol{b}_i)(t) = \omega_x^y b_i(t+n),$$

where $t + n$ is computed mod KW. Let $n = qW + r$ with $0 \leq r < W$. Then, from (42), RHS of the above becomes:

$$\begin{aligned} \omega_x^y b_i(t + qW + r) &= \omega_x^y \omega_K^{iq} b_i(t+r) \\ &= \omega_{xK}^{yK+xiq} b_i(t+r). \end{aligned}$$

Therefore, when we take $x' \triangleq xK$, $y' = yK + xiq$ and $n' \triangleq r$, we end the proof.

b) Since the family $\mathcal{B}$ is uncorrelated, any two distinct sequences $\boldsymbol{b}_i$ and $\boldsymbol{b}_j$ in $\mathcal{B}$ are distinct under cyclic shifts and constant multiples. Therefore, it is sufficient to show that for any $i \in \{0, 1, ..., K-1\}$, any two sequences of $\boldsymbol{b}_i$ obtained by applying different left cyclic shifts within the range 0 to $W-1$ or different constant multiples are distinct. It is obvious since each $\boldsymbol{b}_i$ has zone width W. ∎

REFERENCES

[1] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 36.211 v. 17.2.0, 2022.

[2] A. K. Brodzik, "On Certain Sets of Polyphase Sequences with Sparse and Highly Structured Zak and Fourier Transforms," *IEEE Transactions on Information Theory*, vol. 59, no. 10, pp. 6907–6916, 2013.

[3] A. K. Brodzik, "Polyphase Golay Sequences with Semi-Polyphase Fourier Transform and All-Zero Crosscorrelation: Construction B," in *Excursions in Harmonic Analysis*, Volume 3. Springer, 2015, pp. 211–229.

[4] F. Berggren and B. M. Popović, "Permutation Polynomial Interleaved Zadoff-Chu Sequences," *IEEE Transactions on Information Theory*, vol. 70, no. 8, pp. 6068–6075, 2024.

[5] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Transactions on Information Theory*, vol. IT-18, pp. 531-532, July 1972.

[6] H. Chung and P. V. Kumar, "A New General Construction for Generalized Bent Functions," *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 206–209, 1989.

[7] C. Y. Chen and S. W. Wu, "Golay complementary sequence sets with large zero correlation zones," *IEEE Transactions on Communications*, vol. 66, no. 11, pp. 5197–5204, 2018.

[8] P. Z. Fan, N. Suehiro, N. Kuroyanagi and X. M. Deng, "A Class of Binary Sequences with Zero Correlation Zone," *Electronics Letters*, vol. 35, no. 10, pp. 777–779, 1999.

[9] P. Z. Fan and M. Darnell, *Sequence design for communications applications*, Hoboken, NJ, USA: Wiley, 1996.

[10] Q. Fang and Z. Wang, "A Note on "Optimum Sets of Interference-Free Sequences with Zero Autocorrelation Zone," *arXiv:2202.13764*, 2022.

[11] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar.* Cambridge University Press, 2005.

[12] G. Gong, "Theory and Applications of q-ary Interleaved Sequences," *IEEE Transactions on Information Theory*, vol. 41, no. 2, pp. 400–411, 1995.

[13] Z. Gu, Z. Zhou, A. R. Adhikary, Y. Feng, and P. Fan, "Asymptotically optimal Golay-ZCZ sequence sets with flexible length," *Chinese Journal of Electronics*, vol. 32, no. 4, 806-820, 2023.

[14] G. Kim and H.-Y. Song, "Almost Perfect Sequence Family with Perfect Crosscorrelation," in *Proceedings of 2020 International Symposium on Information Theory and Its Applications (ISITA)*, pp. 456-–459, 2020.

[15] G. Kim, H. Choi, D. Kim, X. Jin, W. Kim, and H.-Y. Song, "Optimal Uncorrelated Polyphase ZCZ Sequences over an Alphabet of Minimum Size," presented at the 2023 IEEE International Symposium on Information Theory (ISIT 2023), Taipei International Convention Center, Taipei, Taiwan, Jun. 25–30, 2023.

[16] N. Kumar, S. Majhi, and A. K. Upadhyay, "A direct construction of complete complementary code with zero correlation zone property for

prime-power length," *Cryptography and Communications*, vol. 16, no. 2, pp. 403–426, 2024.
[17] G. Kim and H.-Y. Song, "The Unique Form of the Uncorrelated Optimal ZCZ Sequence Families," presented at the 2024 IEEE International Symposium on Information Theory (ISIT 2024), Athenaeum Intercontinental Athens Hotel, Athens, Greece, July 7–12, 2024.
[18] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized Bent Functions and Their Properties," *Journal of Combinatorial Theory, Series A*, vol. 40, no. 1, pp. 90–107, 1985.
[19] A. Milewski, "Periodic Sequences with Optimal Properties for Channel Estimation and Fast Start-up Equalization," *IBM Journal of Research and Development*, vol. 27, no. 5, pp. 426–431, 1983.
[20] W. H. Mow, "A unified construction of perfect polyphase sequences," In *Proceedings of 1995 IEEE International Symposium on Information Theory (ISIT)*, pp.459, 1995.
[21] W. H. Mow, "A New Unified Construction of Perfect Root-of-unity Sequences" In *Proceedings of 1995 International Symposium on Spread Spectrum Techniques and Applications (ISSSTA)*, vol. 3, pp. 955–959, 1996.
[22] C. Y. Pai, Y. J. Lin, and C. Y. Chen, "Optimal and almost-optimal Golay-ZCZ sequence sets with bounded PAPRs," *IEEE Transactions on Communications*, vol. 71, no. 2, pp. 728–740, 2023.
[23] K.-H. Park, H.-Y. Song, D. S. Kim, and S. W. Golomb, "The p-ary Fermat-quotient Sequences of period p^2 has the PERFECT autocorrelation," presented at the Information Theory and its Applications (ITA 2016), UCSD, San Diego, Jan.31-Feb.5, 2016.
[24] K.-H. Park, H.-Y. Song, D. S. Kim, and S. W. Golomb, "Optimal Families of Perfect Polyphase Sequences from the Array Structure of Fermat-Quotient Sequences," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 1076–1086, 2016.
[25] S. M. Patole, M. Torlak, D. Wang, and M. Ali, "Automotive Radars: A Review of Signal Processing Techniques," *IEEE Signal Processing Magazine*, vol. 34, no. 2, pp. 22–35, 2017.
[26] B. M. Popović, "Generalized Chirp-like Polyphase Sequences with Optimum Correlation Properties," *IEEE Transactions on Information Theory*, vol. 38, no. 4, pp. 1406–1409, 1992.
[27] B. M. Popović, "Optimum Sets of Interference-Free Sequences with Zero Autocorrelation Zones," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2876–2882, 2018.
[28] H. J. Ryser, *Combinatorial mathematics*, American Mathematical Society, 1963.
[29] N. Rajamohan and A. P. Kannu, "Downlink Synchronization Techniques for Heterogeneous Cellular Networks," *IEEE Transactions on Communications*, vol. 63, no. 11, pp. 4448–4460, 2015.
[30] M. K. Song and H.-Y. Song, "New Framework for Sequences with Perfect Autocorrelation and Optimal Crosscorrelation," *IEEE Transactions on Information Theory*, vol. 67, no. 11, pp. 7490–7500, 2021.
[31] N. Suehiro, "A Signal Design without Co-Channel Interference for Approximately Synchronized CDMA Systems," *IEEE Journal on Selected Areas in Communications*, vol. 12, no. 5, pp. 837–841, 1994.
[32] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower Bounds on Correlation of Spreading Sequence set with Low or Zero Correlation Zone," *Electronics Letters*, vol. 36, no. 6, pp. 1–2, 2000.
[33] X. Tang and G. Gong, "New Constructions of Binary Sequences with Optimal Autocorrelation Value/Magnitude," *IEEE Transactions on Information Theory*, vol. 56, no. 3, pp. 1278–1286, 2010.
[34] H. Torii, T. Matsumoto, and M. Nakamura, "Optimal Polyphase Asymmetric ZCZ Sequence Sets including Uncorrelated Sequences," *Journal of Signal Processing*, vol. 16, no. 6, pp. 487–494, 2012.
[35] L-S. Tsai and Y. T. Su, "Transform domain approach for sequence design and its applications," *IEEE Journal on Selected Areas in Communications*, vol.24, no.1, pp. 75–83, 2005.
[36] W. Yuan and P. Fan, "Implicit MIMO Channel Estimation without de-Offset Based on ZCZ Training Sequences," *IEEE Signal Processing Letters*, vol. 13, no. 9, pp. 521–524, 2006.
[37] D. Zhang, "Zero Correlation Zone Sequences from a Unified Construction of Perfect Polyphase Sequences," In *Proceedings of 2019 IEEE International Symposium on Information Theory (ISIT)*, pp. 2269–2273, 2019.
[38] Z. Zhou, Z. Pan, and X. Tang, "New Families of Optimal Zero Correlation Zone Sequences Based on Interleaved Technique and Perfect Sequences," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer sciences*, vol. 91, no. 12, pp. 3691–3697, 2008.

GANGSAN KIM (student member '18 - member '25) received his BS and PhD degrees in electronic engineering from Yonsei University, Seoul, South Korea, in 2016 and 2025, respectively. In 2022, he served as an AI Science and Technology Soldier at Republic of Korea Army Training and Doctrine Command, where he focused on quantum devices and quantum information theory. He is currently a postdoctoral fellow in the research group of Prof. Hong-Yeop Song at Yonsei University. His area of research interest includes coding theory, PN sequences, related discrete mathematics and their applications to digital communication systems.

JAEHEE NOH recently works as a senior researcher at Korea Aerospace Research Institute (KARI). She received B.S., M.S. and Ph.D. degrees from Chungnam National University, Department of Electronic Engineering in 2017, 2019 and 2022. Her research interests include designing the satellite navigation signal, GNSS receiver, anti-spoofing techniques and navigation message authentication.

HONG-YEOP SONG (student member '85 - member '92 - senior member '07) received the BS degree in electronic engineering from Yonsei University, Seoul, South Korea, in 1984, and the MSEE and PhD degrees from the University of Southern California, Los Angeles, CA, USA, in 1986 and 1991, respectively. He spent two years as a Research Associate at USC and then two years as a Senior Engineer in Qualcomm Inc., San Diego, CA. Since September 1995, he has been with the Department of Electrical and Electronic Engineering, Yonsei University. His research interests include digital communications and channel coding, design and analysis of various pseudo-random sequences for communications and cryptography. He is a member of National Academy of Engineering of Korea (NAEK), Mathematical Association of America (MAA), Korean Mathematical Society (KMS), KICS, IEIE and KIISC. He was awarded the 2017 Special Contribution Award from Korean Mathematical Society and the 2021 S.J.Choi Award from the Korean Government. He has been serving for IEEE IT Society Seoul Chapter as the Chair from 2009 to 2016. He served as the General Co-Chair for IEEE ITW 2015, Jeju, South Korea.